A Study of the Awareness on Cyber Safety and Security among Secondary Students

(Class IX to XII)

Principal Investigator
Dr. Angel Rathnabai

March, 2024

Central Institute of Educational Technology
National Council of Educational Research and Training
Sri Auribondo Marg, NCERT Campus, New Delhi, Delhi- 110016

A STUDY ON THE AWARENESS OF CYBER SAFETY AND SECURITY AMONG SECONDARY-STAGE STUDENTS (CLASS IX TO XII)

Research Report

Principal Investigator

Dr. Angel Rathnabai

Central Institute of Educational Technology

National Council of Educational Research and Training

Sri Aurobindo Marg

New Delhi-110016

DECLARATION

I declare that this research entitled "**A Study on the Awareness of Cyber Safety and Security among Secondary-Stage Students (Class IX To XII)**" has been taken up as a part of the **PAC 20.05 project.**

Principal Investigator
Dr. Angel Rathnabai S
CIET-NCERT

Head (DICT)
Prof. Indu Kumar
CIET-NCERT

Joint Director
Prof. Amarendra P.Behera
CIET-NCERT

DECLARATION

I declare that this research entitled **"A Study on the Awareness of Cyber Safety and Security among Secondary-Stage Students (Class IX To XII)"** has been taken up as a part of the **PAC 20.05 project.**

Principal Investigator
Dr. Angel Rathnabai S
CIET-NCERT

Head (DICT)
Prof. Indu Kumar
CIET-NCERT

Joint Director
Prof. Amarendra P.Behera
CIET-NCERT

ACKNOWLEDGMENT

We would like to sincerely thank Prof. Amarendra P. Behra, Joint Director, and Prof. Indu Kumar, Head, DICT & TD, Central Institute of Educational Technology (CIET), NCERT, New Delhi, for their valuable expertise and guidance throughout this project. Their leadership played a key role in shaping our work and ensuring its quality.

We also want to recognize the important contributions of the resource persons and experts whose insights and hard work were essential in the research.

I am also profoundly appreciative of the participants of the research. Their active engagement and enthusiasm were crucial in bringing this research to life. Their feedback and reflections provided valuable insights that have significantly contributed to the findings of this report.

Table of Content

CHAPTER 1: INTRODUCTION

1.1 Overview of Digital Landscape in India

India’s digital landscape has seen transformative growth with widespread internet access and the proliferation of mobile technology, reshaping various aspects of daily life and education. A wide range of digital tools and materials are now easier to access, which has an impact on how education is provided and received. This increase in internet penetration is powered by reasonably priced cell phones and data plans. The National Education Policy (NEP) 2020 and the Digital India campaign, two government programs aimed at enhancing digital infrastructure and incorporating technology into teaching methods, provide support for this digital transformation. Nevertheless, despite these developments, more people are using digital platforms, which increases their vulnerability to online dangers including phishing, cyberbullying, and data breaches. It is essential to comprehend secondary-stage students' awareness of cyber safety and security because they are especially susceptible to these hazards (classes IX to XII). This study aims to examine the efficacy of current educational initiatives in equipping students to face online dangers and to gauge how effectively these pupils understand cyber safety principles, including safe internet habits and privacy protection.

1.2 Importance of Cyber Safety and Security in the Context of Growing Internet among Students

The significance of cyber safety and security is becoming more and more apparent as the number of pupils using the internet rises. Increased access to a wealth of information and interactive teaching tools are only two benefits of increased digital connectivity for education. But students are also more vulnerable to online threats because of this increased connectedness, such as phishing, cyberbullying, and data breaches. Cyber safety education must be given top priority in order to reduce these threats. Safeguarding students' digital well-being requires making sure they know how to utilize privacy settings wisely, secure their personal information, and behave appropriately when navigating online environments. In addition, encouraging responsible digital citizenship fosters polite online interactions and works to stop harmful behaviours like cyberbullying. Students who receive more critical thinking instruction are better able to distinguish reliable information from false information and stay away from internet scams. Incorporating cyber safety education into the curriculum benefits kids in two ways: it keeps them safe and helps them use digital technologies effectively and confidently, which helps them succeed academically and grow in a connected society. Overall, integrating cyber safety education into the curriculum is vital for safeguarding students in the digital age, ensuring they can navigate online environments securely and responsibly.

1.3 Emerging Cyber Threats and the Impact on Students

As digital technology becomes increasingly integrated into daily life, there is a rising number of cyber threats that students must deal with, which could seriously impact their safety and

well-being. New and dangerous cyber threats that target students' personal information and academic data include ransomware, malware, and phishing scams. Phishing scams frequently deceive students into divulging personal information, which can result in identity theft or monetary loss. Malware and ransomware have the ability to infiltrate personal devices and school networks, interfering with academic activity and possibly leading to data loss.

Additionally, cyberbullying has become a pervasive issue, with students experiencing harassment and bullying through digital platforms, which can lead to severe emotional and psychological distress. Students may find it more difficult to leave dangerous situations because of the anonymity and reach of online contacts, which can intensify the negative impacts of bullying. Students must be aware of and take precautions against these concerns because the presence of exploitative content and online predators exacerbates these risks. The significance of these new cyber threats highlights the critical need for thorough cyber safety education, giving pupils the know-how and abilities to safely traverse the digital environment and reduce hazards.

Emerging new and sophisticated threats include deepfake technology, which can produce deceptive and harmful content that could affect students' reputations and mental health; social engineering attacks, which take advantage of people's trust and vulnerability by tricking them into disclosing private information; and the growth of dark web activities and illicit online communities, which expose students to unlawful and dangerous content, including harmful practices and extremist ideologies.

The prevalence of influencer fraud and other fraudulent schemes that take advantage of students' hopes and dreams can lead to both monetary losses and psychological suffering. Inappropriate content may be exposed to students or personal data may be collected without authorization through exploitative internet games and applications. The necessity for proactive cyber safety education is highlighted by the growing sophistication of these threats. This will ensure that students are aware of the hazards involved and have the knowledge and resources necessary to protect themselves in the digital era. Teachers and parents may help students navigate the internet safely and responsibly by addressing these new threats.

1.4 Statement of the Problem

The secondary school students of India are increasingly exposed to cyberspace owing to rapid digitalization. With the increasing use of internet-connected devices and social media platforms, students get exposed to various kinds of cyber threats. In this context, their awareness about cyber safety and security is of paramount importance. This study intends to check the awareness of secondary students about cybersafety and security of secondary students studying in various schools of India. An understanding about the students' awareness would be helpful to promote cybersafety and security skills among the learners so that they can be safeguarded against cyber threats. In this context, the current research work has been undertaken and is entitled as '*A Study on the Awareness of Cyber Safety and Security Among Secondary Stage Students (Class IX to XII)*.

1.5 Operational Definition of the Key Terms

1.5.1 Awareness

Awareness is the quality or state of being aware: knowledge and understanding that something is happening or exists (Merriam-Webster, 2024). In this study, an awareness for teachers is referred to as an organized educational programme designed to give instructors the knowledge, skills, and practices they need to comprehend and apply cyber safety and security measures in learning environments.

1.5.2 Cyber Safety and Security

According to Merriam-Webster, cyber safety is the safe practices when using the Internet to prevent personal attacks or criminal activity. Cybersecurity is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks (Kaspersky, 2024). In this study, Cyber Safety and Security refer to teachers who understand how to keep themselves and their students safe online and are practising cyber safety and security. It involves educating students on how to be responsible online, accessing the internet safely, creating strong passwords, and identifying and addressing online threats including scams and cyberbullying.

1.5.3 Secondary School Students in India

Secondary school students are defined as individuals who are enrolled in grades IX through XII within the Indian educational system. These students typically range in age from approximately 14 to 18 years.

1.6 Variables of the Study

Variables are the factors involved in addressing the research problem, which leads to the closure of the research gap. These attributes ought to impact one another. The current study investigates secondary students' levels of awareness of cyber safety and security. Hence, the following independent and dependent variables were identified for the investigation of the study:

- **Independent Variable**

  An independent variable is a variable that has been manipulated. The independent variable is purposely manipulated during observation to determine its relationship with the dependent variable. So the demographic factors Gender, Standard, States/UTs, Type of School, Locality of the school and Medium of Instruction are considered as independent variables.

- **Dependent Variable**

  The dependent variable is the level of awareness of cyber safety and security among secondary-stage students. This variable represents the degree to which students understand and are informed about various aspects of cyber safety and security, such as recognizing cyber threats, understanding safe online practices, and knowing how to protect personal information online. This awareness can be measured through surveys,

questionnaires, or assessments designed to evaluate students' knowledge and attitudes towards cyber safety and security issues.

1.7 Research Questions

1. What is the awareness level of secondary students on cyber safety and security?
2. What are the dimensions in which secondary students lack awareness of cyber safety and security?

1.8 Objectives of the Study

1. To evaluate the level of awareness and understanding of cyber safety and security among secondary-stage students.
2. To study the difference in awareness on cyber safety and security among secondary school students with respect to various subgroups.
3. To study the difference in different dimensions of cyber safety and security awareness among secondary school students with respect to various subgroups.

1.9 Hypothesis of the Study

To undertake a meaningful analysis, the following hypotheses were proposed. There are 16 hypotheses which were clubbed under three broad hypotheses as given below:

H_1: There is no significant difference in the mean score of cyber safety and security awareness of secondary students with respect to their/ the

1. Access to Internet at home
2. Possession of personal email ID
3. Participation in ICT courses
4. Availability of digital devices at home
5. Availability of own digital devices
6. Possession of personal social media account
7. Duration of use of devices per day
8. Perception about excessive screen time

H_2: There is no significant difference in the mean score of cyber safety and security awareness of secondary students with respect to

1. Locale of the school
2. Gender of the student
3. Standard in which the students are studying
4. Type of school

H_3: There is no significant difference in the mean score of different dimensions of cyber safety and security awareness of secondary students with respect to

1. Locale of the school
2. Gender of the student
3. Standard in which the students are studying
4. Type of school

1.10 Research Methodology

1.10.1 Research Design

The study utilized a survey method, a quantitative research technique, to investigate students' awareness of cyber safety and security on a national scale. This approach was chosen to explore the current level of understanding among secondary-stage students regarding cyber threats and protective measures. By employing descriptive and inferential statistics, the survey method provided a comprehensive view of students' awareness across different regions. The use of surveys allowed the researcher to gather data on students' knowledge and attitudes toward cyber safety, offering valuable insights into the prevailing level of awareness and identifying areas that may require further educational intervention or policy development. This method proved effective in capturing a broad spectrum of information, essential for assessing and improving cyber safety education nationwide.

1.10.2 Population of the Study

The population of the present study is all the secondary school students studying in various Government, Private, or Aided schools, from all 28 Indian States and 8 Union Territories. There are about 6.7 crore students enrolled in secondary education in the 2023-24 session (MoE, 2021) and all of them were considered as the population of the present study.

1.10.3 Sampling Technique

A convenience sampling method was used to collect data from secondary school students. The first stage was the selection of states/UTs and autonomous bodies for collecting data. In the first stage, it was decided to collect data from students of class IX to XII studying in all boards i.e., Boards of all 36 States/UTs and CBSE. In the second stage, the schools were selected. All the schools affiliated to the boards of States/UTs and the following schools affiliated to the CBSE board were selected: 1) KVS, 2) NVS, 3) Sainik Schools, 4) AESS, 5) EMRS, 6) Private schools affiliated to CBSE. In the third stage, convenient sampling was employed to select the sample of the study.

1.10.4 Sample of the Study

The sample consists of students studying in standard IX to XII in schools at States/UTs and autonomous organizations.

1.10.5 Research Tool

A cyber safety and security awareness scale covering five dimensions of cyber safety and security was constructed. Validity and reliability was achieved by going through pilot testing. The research tool was developed in English and also translated into Hindi.

1.10.6 Data Collection

An online-based survey was used to collect the data. The research tool was shared through the school authorities and in turn data was collected from the students.

1.10.7 Data Analysis

The quantitative data was analyzed under descriptive and inferential parameters. MS-Excel was used for descriptive analysis, and SPSS Software was used for inferential analysis, such as t-test, ANOVA, etc.

1.11 Need and Significance of the Study

The study on the awareness of cyber safety and security among secondary-stage students (Class IX to XII) is essential in today's digital age, where adolescents are increasingly immersed in online environments through educational tools, social media, and various digital platforms. As these students navigate their academic and social lives, they are exposed to a range of cyber risks, including cyberbullying, phishing scams, and privacy breaches. This research seeks to evaluate their current level of understanding and preparedness regarding these threats. By identifying gaps in their knowledge and awareness, the study aims to provide valuable insights that can guide the development of more effective educational programs and policies tailored to their specific needs. Such insights will be instrumental in crafting targeted interventions that empower students to practice safe online behaviors, protect their personal information, and respond appropriately to cyber threats. Furthermore, the findings will serve as a resource for educators, parents, and policymakers, offering a basis for enhancing digital safety curricula and fostering a culture of responsible digital citizenship. Ultimately, the study's significance lies in its potential to improve students' online safety and contribute to a more secure and informed digital community.

1.12 Scope of the Study

Research on students' cyber safety and security can have a wide scope and cover a variety of topics linked to making sure students are safe and secure online. Children are currently facing a wide range of cyber safety and security concerns and risks, including malware, phishing scams, cyberbullying, online predators, and different cyberattacks directed exclusively at children. These hazards not only jeopardize students' personal information but also endanger their mental and emotional well-being, academic performance, and overall development. To address these issues, it is critical to assess the efficacy of current cyber safety and security awareness and education programmes for children, such as school-based initiatives, online resources, and seminars. Furthermore, knowing the cyber safety and security measures students use, such as password management and social media privacy settings, is critical for encouraging safer online behaviour. Parental engagement and aid support students' cyber safety and security activities. Examining legislative and legal frameworks at the local, national, and international levels, including data privacy legislation and online platform limits, is critical for providing a secure environment for students online. Technological solutions such as parental control software, firewalls, antivirus software, and content screening technologies can help students stay safe online. Cultural norms, socioeconomic determinants, and digital literacy levels all have a substantial influence on pupils' capacity to detect online dangers and adopt cyber safety and security measures, emphasizing the necessity of considering these aspects. We can collaboratively create a safer online environment for students by describing best practices and making recommendations to educational institutions, guardians, politicians, and

technology corporations. Finally, anticipating future trends and difficulties in cyber safety and security for students is critical in predicting technical advancements, emerging cyber dangers, and the transforming implications of the digital revolution on classroom dynamics.

1.13 Delimitations of the Study

Delimitations help focus the research by specifying what aspects will be included and excluded from the investigation. Here are some probable delimitations for this study:

- **Age Range:** The study focused solely on students in grades 9–12, omitting younger or older age groups. This delimitation ensures a specific assessment of cyber safety and security awareness within the context of secondary school.
- **Educational Setting:** Students enrolled in government, private, and aided schools were the only subjects of the study; homeschoolers and participants in alternative education programs were not included. An investigation in a more homogeneous sample and context was made possible by this delimitation.
- **Dimensions of Cyber Safety and Security:** The study concentrated only on five dimensions of cyber safety and security namely Technical, Psychological, Physical, Legal, and Socio-ethical. This boundary guarantees a targeted analysis of the most critical cyber safety and security concerns that affect the intended sample.
- **Research Methodology:** To investigate students' awareness of cyber safety and security, the study used specialized research techniques, such as online surveys through Google Forms.
- **Language coverage:** The tool of the study was prepared in English and translated only in Hindi.

1.14 Organization of the Research Report

The research report is organized into six chapters. The first chapter, Introduction, presents the need and significance of the study, statement of the problem, the definition of the key terms, variables of the study, objectives of the study, the hypotheses of the study, methodology, scope and delimitations of the study. The second chapter is a review of related literature, a theoretical overview and studies related to cyber safety and security. The third chapter, Methodology, presents a detailed account of the methodology, including descriptions of the method of the study, design of the study, variables of the study, tools used for the study, description of tools, population and sample selected for the study, procedures for data collection and the statistical techniques used for analysis. The fourth chapter, Analysis and Interpretations, deals with the analysis of data in detail. This chapter includes preliminary analysis, percentage analysis, mean difference analysis, and correlation analysis. The fifth chapter, Summary of Findings and Conclusions, contains a summary of findings, tenability of hypotheses, the relationship of results to existing studies, limitations of the study, suggestions, recommendations and educational implications for further research, and conclusions.

CHAPTER 2: REVIEW OF RELATED LITERATURE

2.1 Introduction

Fundamentally, research is an ongoing dialogue – a scientific effort to expand the limits of human understanding. It is essential to carefully review the current debate before starting any research. Here, the literature review assumes a central role, serving as a link between existing knowledge and forthcoming research. Its significance cannot be emphasized since it provides a solid basis for thorough study and has many advantages. Examining the body of prior research is essential when it comes to educational research since it serves as the foundation for novel and vital findings. Examining relevant literature is a crucial first step, compass, and guidance for academic research projects. First of all, it provides a thorough grasp of the existing environment, including recognized gaps, accepted ideas, and established information. In addition, this enables ongoing research to place the findings within the broader discussion carefully. Moreover, a critical examination of earlier research refines the methodology by highlighting both possible advantages and limitations. It also generates new ideas by pointing out places where the body of knowledge is lacking or ambiguous, which opens the door for special contributions. In the end, a comprehensive study promotes scholarly progress within an area. The following are the reviews from the national and international research studies which were carried out on awareness of cyber safety and security among students.

2.2 Review Related Literature

Jalil et al. (2024) proposed a cyber-awareness programme to help students learn about cybersecurity and control the danger of cyber-attacks. The process is divided into four phases: initiation and planning, module development, implementation, and evaluation. Descriptive and statistical studies demonstrate that participants' knowledge of cyber security dangers and risks increased after participating in the programme. Finally, this programme met its goals of raising cyber security knowledge and encouraging participants to use the internet safely. These findings indicate that similar programmes might be used to raise cybersecurity awareness and promote safe internet use among students.

Alfalah (2023) evaluated how different aspects of cyber security perception affected students' views about using learning management systems (LMS) and how much Internet security awareness may impact these connections. The study employed a quantitative methodology, collecting 261 responses from students in the Kingdom of Saudi Arabia using a survey questionnaire. Analysis revealed that attitudes are influenced by several important factors, including perceived privacy, trust in the Internet, trust in the university, and perceived cyber risk. All of these correlations are mitigated by awareness of Internet security.

Masenya (2023) investigated the students' awareness and understanding of cyber ethical conduct at South African HEIs. Using the content analysis approach, this study also looked into the variables that contribute to unethical cyber activity and the cyber security measures that stop it among students in HEIs in South Africa. Ethical theories such as consequentialism, deontology, virtue ethics, and Kohlberg's theory of moral growth also served as a guide for the

research. While most students at Higher Education Institutions (HEIs) are aware of unethical online behavior, such as fraud, hacking, cyberbullying, and pornography, it seems that these institutions lack a cooperative approach to computer security best practices and cyber ethical behavior education.

Wei-Kocsis et al. (2023) presented a fresh proactive and collaborative learning paradigm for educating and training a qualified cyber workforce in this new era of security breaches, privacy abuses, and artificial intelligence. This learning paradigm was developed using the educational principles of technology-mediated learning and social constructivism. The findings indicated that, while the research is still ongoing, the prototype learning paradigm has demonstrated promising outcomes in enhancing learners' engagement in applied AI learning.

Alsharida et al. (2023) carried out a systematic review to provide multiple perspectives on human cybersecurity behavior by evaluating and synthesizing cybersecurity theories/models, independent variables, target variables, moderators, methodologies, participants, units of analysis, technologies/services, countries, and domains. Of the 2936 papers gathered, 93 studies satisfied the inclusion criteria and were extensively examined. The major findings suggested that the protection motivation theory (PMT) and the theory of planned behavior (TPB) were the most widely used theories in the studied literature. 76% of the papers reviewed did not use a moderator to investigate the associations between predictors and target variables. The majority of the studies were done on an individual basis, mostly involving students and end users. Social media and mobile devices were the most often studied technologies for human cybersecurity behavior.

Baraković and Baraković (2023) assessed how the COVID-19 pandemic conditions affected the outcomes related to cyber hygiene, such as awareness, behavior, and knowledge. The goal was to assess and contrast university students' levels of cyber hygiene before and after the COVID-19 epidemic. The survey study's findings show that university students' awareness, behavior, and knowledge of cyber hygiene have changed as a result of the COVID-19 epidemic.

Shah and Agarwal (2023) recommended Cyber Suraksha, a tabletop card game, to raise threat awareness and encourage users to implement recommended security precautions for smartphone users. The risk behavior diagnostic scale was used to collect responses from participants in both the control and intervention groups. The results showed that the game was entertaining and fun. The Cyber Suraksha game efficiently convinces users to implement the recommended security controls for the targeted conduct. The findings show that individuals in the intervention group are 2.65 times more likely to follow suggested behavior. The study's findings support the usefulness of hope and fear appeals in raising cybersecurity awareness.

Ahmed et al. (2023) assessed the level of cyber security knowledge among graduate and undergraduate students at five institutions in Mogadishu. A questionnaire was used to collect data from 250 pupils. The cross-tabulation results revealed that there was a considerable variance in cybersecurity awareness levels among universities. The findings revealed that SIMAD and Jamhuriya University students were vulnerable to malware assaults, whereas SIU students battled with password strength and social network abuse. Students in Mogadishu were

subjected to phishing and virus assaults, while students at UNISO encountered virus attacks as well as password strength concerns.

Sussman (2023**)** explored cybersecurity through the lens of the National Institute of Standards and Technology (NIST) framework. This strategy employs the topics of identify, protect, detect, respond, and recover to foster an atmosphere of everyday cyber safety. The chapter then describes how cybercriminals affect people's behavior. This knowledge will assist pupils in recognizing cybercriminal behavior and being more cyber secure.

Ellala et al. (2023) assessed how much knowledge a sample of superior and regular students in the education department at Al Ain University had about cyber security. Students of all genders made up the study sample. According to the scale's total score, both gifted and average students in the faculty of education had a high degree of knowledge about cyber security. The findings showed that while the degree of cyber security awareness attributed to the variable of gender (male, female) did not show statistically significant differences, the level of awareness assigned to the variable of student type (superior, ordinary) did show statistically significant differences, with exceptional students showing a greater degree of awareness.

Huraj et al. (2023) investigated university students' attitudes and awareness levels of cyber security. The survey, which compares students' opinions in two subjects' computer science and media studies on a sample of 570 students, is based on empirical data. According to the statistical analysis results, the responses from the surveys of students in the two fields exhibit both parallels and contrasts.

Alammari et al. (2022) validated a fuzzy linguistic group decision-making technique to assess cybersecurity degree programme competencies regarding knowledge, skills, and abilities (KSAs). This demonstrates the need for cybersecurity knowledge, as well as technical skills and human capabilities, for cybersecurity professionals.

Erendor and Yildirim (2022) investigated to determine to what degree Kyrgyz-Turkish Manas University students are informed about cybersecurity throughout the remote education procedure. The poll included 517 students from all university faculties at the undergraduate, graduate, and PhD levels. The findings revealed that the kids knew nothing about cybersecurity or the consequences of cyberattacks in general. An investigation of cybersecurity awareness was conducted by asking questions about harmful software, password security, and social media security. It has been established that kids have little cybersecurity awareness. It has been further decided that cybersecurity education should be provided to kids in order to protect them from being victims of cyberattacks and to help them utilize the internet more efficiently.

Raju et al. (2022) investigated students' cybersecurity awareness. The study is crucial since it focuses on flaws and educates pupils about being cyber victims. A set of questionnaires was distributed to 110 students to gather data. Open-ended and closed-ended questions provided numbers and figures, which aided in data collection. Descriptive analysis reveals that many pupils are aware of and understand cyber security, cyberattacks, and cyberbullying.

Mohammed and Bamasoud (2022) addressed how important it is to raise cyber security knowledge among students in order to prevent cyber risks. Cybersecurity awareness is one of the aspects of cybersecurity controls that strive to raise knowledge of cybersecurity threats and

hazards, as well as to foster a healthy cybersecurity culture. Furthermore, cybersecurity awareness is a vital aspect of preserving the security and privacy of sensitive information assets. Students' understanding of cybersecurity, its hazards, and risks improves students' references to action when faced with cybercrime to safeguard information and technological assets to attain secure cyberspace.

Alqahtani (2022) analyzed university students' cybersecurity knowledge using three key criteria: password security, browser security, and social media. The survey generated up to 450 replies. It discovered that knowledge of password security, browser security, and social media activity had a substantial impact on students' cybersecurity awareness. Overall, pupils have recognized the need for cybersecurity knowledge.

Tsimtsiou et al. (2021) evaluated the teenagers' perceptions of this school-based intervention. A student sample was drawn using a multistage stratified random sampling procedure based on geography and school grade level (middle and high school). Students aged 12 to 18 received an interactive presentation in their classes about the amount of time spent online, the usage of social networks, and the available support services. Four hundred and sixty-two kids (90.7% response rate, 246 middle, 216 high school) completed the assessment form. Younger children, particularly those in their first year of middle school, scored considerably higher in all six measures utilized in the evaluation of this intervention than all older participants.

Aljohni et al. (2021) analyzed students' current levels of cybersecurity awareness (CSA). The cybersecurity students' awareness level questionnaire was derived from many prior cybersecurity awareness initiatives. 136 students took part in the survey. The study's findings demonstrate that there is no substantial difference in cybersecurity knowledge levels between male and female pupils, although females are slightly more concerned about cybersecurity. However, students in computer and information technology disciplines are more knowledgeable than others. Furthermore, urban pupils demonstrated higher levels of cybersecurity awareness than students from distant places. The survey findings show that the study model helped assess students' awareness.

Ahmad and Othman (2019) carried out a literature study to examine knowledge of information privacy among the younger generation in particular. According to the findings, a lack of awareness of the principles of Internet knowledge has increased occurrences of Internet scams, online harassment, cross-site scripting, and identity theft. The study proposed that a thorough and suitable legislative framework be built on an ongoing basis to fight the concerns.

Tsokoto et al. (2019) performed action research to establish a plan for improving e-safety among Zimbabwean students. The data was gathered using an online questionnaire, group discussions, and student observations. The study was continuous, with two cycles completed, and the results led to the development of a strategy based on the WHAT, WHO, and HOW.

Musharraf et al. (2019) investigated both general and Internet and Communication Technology (ICT) self-efficacy in several domains. Students were surveyed on cyberbullying/ victimization, general self-efficacy (GSE), ICT self-efficacy, traditional bullying/

victimization, ICT usage, social desirability, and demographics. In terms of gender, the data revealed that females were more likely to be victimized, whilst males were more likely to perpetrate both conventional and cyberbullying.

Koyuncu and Pusatli (2019) evaluated smartphone users' awareness levels for several security-related characteristics and compared them to other user groups based on demographic data. It is based on a survey of a population of a wide variety of ages and educational levels. According to the results, participants' awareness levels are often poor and require significant development. In terms of age, the oldest group scores the lowest, followed by the youngest group. Overall, education has a favorable influence on awareness.

Mousa (2019) researched cybersecurity awareness among students. The researcher employed a questionnaire and developed a study model based on the customized TPB model. The poll included 140 students from both ICT and non-ICT-related professions. The findings revealed a lack of awareness of cyber security risks, with pupils having just a modest understanding of the subject. A proposal is made to launch and promote cybersecurity awareness initiatives among students.

Durak et al. (2017) evaluated the impact of Wild Web Woods (WWW), a game designed by the European Council for safe Internet usage, on secondary school pupils' safe Internet use. To measure students' awareness of safe Internet use, 504 students from various areas of Turkey were surveyed. The researchers devised a 25-item questionnaire for the study, which was administered to the students. The data analysis demonstrated that pupils were largely aware of safe Internet use.

Ma et al. (2023) developed and validated a scale for internet literacy intended for high school students. Seventy-four high school students were enlisted in the study, and thirty items covering eight dimensions-self-management, self-image construction, damage control, information processing, critical thinking, cooperation, moral consciousness, and security—were included in the validated scale. The study also suggests potential uses of the scale in an educational setting.

Taking into consideration the variety of individuals in terms of demography, socioeconomic level, and the digital divide, Khan et al. (2023) examined the cyber-security and risky Internet behaviors of undergraduate students from Pakistan. A survey questionnaire was used to gather data. Using multistage stratified sampling in face-to-face interactions, 294 students from six distinct cities in Pakistan were surveyed. According to gender, age, and digital divide characteristics, the results showed considerable disparities in cyber-security posture. Based on cyber-security and risky Internet behaviors, student profiles reveal three categories, the majority of which are characterized by poor cyber-security behavior and a greater inclination towards risk aversion. High-risk-averse behavior is also positively impacted by proactive cyber-security awareness behavior.

Baraba and Tomaš (2022) investigated the variables pertaining to school children's Internet usage and awareness of online safety in the Croatian language. An eighteen-item Croatian questionnaire was prepared and used for data collection. According to the findings, students in urban regions had a greater understanding of the notion of personal data than

students in rural areas (71,2% vs. 47.2%, P=0.038). Pupils do not fully comprehend or are aware of online safety. It draws attention to the necessity of a suitable educational intervention.

Using questionnaires, Macaulay et al. (2020) evaluated the attitudes toward e-safety education, the subjective and objective knowledge of online safety and hazards, and the perceptions of children (N = 329) regarding their safety online. Although most participants felt safe while using the internet and thought they knew a lot about the risks and how to avoid them (subjective knowledge), they were often not very good at defining those risks and how to prevent them specifically (objective knowledge). For boys and younger children in particular, this was true. Taken together, these results imply that while certain children may believe they understand how to be safe online, they may lack objective information that may keep them secure or at least be unable to express it. The study proposed that it is necessary to evaluate children's objective understanding of internet safety and dangers and to give children the right education.

Zulqadri et al. (2022) identified potential security hazards associated with online learning and the steps that may be taken to mitigate these risks. Employing two techniques: literature reviews and web mining, the study found that there are a number of risks associated with using the internet, including viruses, phishing, scams, fraud, cyberbullying, problems with privacy and personal data, and offensive or pornographic content. Additionally, this study offers three crucial measures for safeguarding kids from online dangers while they are learning online: helping them access online resources, educating them about internet safety and personal data protection, and introducing them to digital citizenship and online ethics.

Ahmad et al. (2022) emphasized cybersecurity education in all fields and at all levels. The emphasis is on the following four categories of users: K-12, college, technical professionals, and all other citizens. A curriculum roadmap that incorporates cybersecurity into both technical and nontechnical courses is offered as the foundation for future cyber education planning. The purpose is to teach students and people the notion of cybersecurity, assure their ability to apply cybersecurity principles and expose them to various ways to resolve cybersecurity-related issues.

AlDaajeh et al. (2022) examined national cybersecurity strategic plans (NCSP) from different nations and areas, discussed initiatives to improve cybersecurity curricula and best practices, and looked into the most effective ways to develop engaging cybersecurity education and training programmes to entice people to consider the field for their future careers. Additionally, the study looks at several strategies for matching higher-level strategic objectives with curriculum enhancements for cybersecurity education and training programmes.

Quyen and Lien (2022) carried out a literature evaluation of research on school pupils' digital safety competencies. Studied over 90 academic articles and government records. It demonstrates the need for activities that reinforce knowledge and abilities, as well as reorientation or reinforcing attitudes towards digital safety and the constructive use of new media at home and school. The findings also present chances to further our understanding of the educational processes that occur in the home context in the digital era.

Martin et al. (2021) investigated parents' perceptions of student digital safety based on technology use, time spent, parental worries, and understanding of several digital safety subjects. The researchers evaluated data from 113 parents as part of a survey-based study. Parents stated that their children mostly use the Internet on tablets and computers to view movies, play games, and complete schoolwork. Parents were familiar with the applications and gaps their children used for education and amusement. Regarding time limitations and access restrictions, 40% of parents allow their children to spend 1-2 hours online every day, while 47% establish time constraints. Parents are always concerned about their children's internet safety, with the most pressing issue being their children's exposure to sexual content and interactions with strangers.

Jian and Kamsin (2021) studied ways to use gamification to raise cybersecurity awareness among teens, as well as how a computer game may entice teenagers to learn about cybersecurity. For this study, the quota sampling approach is used with 50 secondary students aged 13 to 15 in Malaysia via an online survey. Three students were chosen at random to participate in the interview session to ensure the reliability of the online survey results. Future studies to enhance cybersecurity awareness would be advised, emphasizing activities that schools must take.

Wahid et al. (2021) established a cybersecurity awareness approach that can protect citizens from online threats. This study uses a quantitative methodology, selecting 300 samples using a convenience sampling strategy. Three factors—organizational, societal, and individual-were shown to influence cybersecurity awareness in the study. The findings showed that whereas social and individual variables were found to be less important to cybersecurity awareness, organizational aspects were shown to be highly associated with cybersecurity awareness.

Dorasamy et al. (2021) performed a qualitative study by interviewing 19 parents with children aged 13 to 17 years to establish their degree of awareness. Results are linked to three major variables of cyber grooming: parental influences, self-efficacy, and self-regulation. The research concluded with findings and suggestions for parents, schools, and the government to be more vigilant against online predators and raise awareness of cyber grooming.

Aldosari et al. (2020) investigated the requirements for digital citizenship among middle and high school pupils in Riyadh, Saudi Arabia. A quantitative survey was used to determine whether components of digital citizenship were available to 394 students. The four areas of digital citizenship, digital identity, ethical behavior, intellectual property, and digital privacy and security were the foundation around which the survey items were constructed. The results showed that students had high levels of Internet self-efficacy and digital citizenship availability in both the first and second domains. The promotion of digital citizenship among middle and high school students should receive more attention, with a focus on educating them about digital identity, cybersecurity, online bullying, intellectual property rights, and appropriate online behavior.

Nkechi et al. (2020) examined cyber safety in junior secondary education. A descriptive survey methodology was employed to gather data from 815 educators. It was shown that teachers had a limited understanding of the issues related to junior secondary school students'

use of the Internet. Additionally, no internet safety tactics are taught to the pupils. According to the study's findings, while the educational system promotes students' use of the internet, it cannot continue to downplay the hazards and let them squander their futures on it.

Podila et al. (2020) created Android applications that addressed cyber-safe practices through run-time permission attacks and malware classes such as scareware, ransomware, spyware, and phishing using social networking apps. The apps were discussed in light of typical users and cybercriminals. Through the use of these applications, an effort will be made to conduct psychological evaluations on young high school students in order to detect cybersecurity dangers, preventing them from being victims of cyberattacks and enhancing their confidence in their ability to pursue a career in cybersecurity.

Fatokun Faith et al. (2020) performed an online survey of 450 students from Malaysian tertiary institutions. The investigation discovered correlations between cybersecurity behavioral variables. Except for perceived severity, all criteria were strongly associated with students' cybersecurity behaviors. The investigation emphasizes the need for increased cybersecurity training and practices at institutions.

Kritzinger (2020) assessed the four primary components of cyber safety—leadership and policies, infrastructure, education, and standards and inspection in order to determine the maturity levels of cyber safety in 24 South African schools. According to the data, there was a marked lack of cyber safety maturity and compliance in all of the study's participating institutions. In an effort to better prepare students for the future, schools in South Africa are beginning to integrate technology into their curricula, but there is a conspicuous dearth of rules, practices, and procedures that promote cyber safety awareness. The study suggested a ten-phase cyber safety strategy as a step-by-step method to enable schools.

Nicolaidou and Venizelou (2020) designed an interactive web-based learning environment and assessed its efficacy and motivating potential for enhancing children's e-safety knowledge. Using a quasi-experimental pre-test post-test control group design, 48 sixth-grade primary school students participated in two 80-minute classes using the web-based learning environment, whereas 25 students in the control group did not utilize it. The experimental group students' favorable sentiments towards the learning environment were established through the analysis of an attitudes questionnaire and student interviews. Results show how well the web-based learning environment, which can be utilized in both formal and casual learning contexts, can motivate students and help them develop their e-safety skills.

Dhaka (2020) evaluated the level of knowledge of cybercrime among Senior Secondary School pupils in the Meerut District, by using a descriptive survey method, based on factors like gender, school type, and area. It was discovered that there are no appreciable differences between the pupils based on their location or gender. Additionally, it was shown that children's understanding of cybercrime varies significantly depending on the kind of school they attend. When compared to students attending government senior secondary schools, the pupils in private senior secondary schools had a greater understanding of cybercrime. Therefore, it is advised that to protect themselves, pupils should be educated to be aware of cybercrime and to abstain from engaging in it.

Erdoğdu et al. (2021) developed and validated the Mobile Information Security Awareness Scale (MISAS), which measures information security awareness, as well as the related literature. The scale was created and verified with the help of 562 students. The MISAS has six criteria and seventeen elements. Backup, instant messaging and navigation, password security, updates, access permissions, and using others' devices were among the reasons found.

Khader et al. (2021) proposed a conceptual Cybersecurity Awareness Framework to guide the adoption of tools to promote students' cybersecurity awareness in any academic setting. This framework consists of components that constantly enhance the development, integration, delivery, and assessment of cybersecurity knowledge within an institution's curriculum.

Omar et al. (2021) developed a malware awareness tool aimed at students. This tool's development followed the Game Development Lifecycle (GDLC) approach. The tool development period began with commencement, progressed to pre-production, production, testing, and beta testing, and concluded with the release phase. The functionality testing revealed that this product was well-received by its target students. The malware awareness tool that was developed increased students' knowledge of malware and increased their understanding of Internet hazards.

Tomczyk and Eger (2020) assessed the group of upper-secondary school students' digital literacy in the area of risks associated with utilizing new media. An eighteen-item diagnostic exam was used in the investigation. The study involved 1693 young people between the ages of 15 and 21. The design of the study was influenced by conventional techniques for evaluating knowledge and skills. The results demonstrated that copyright-related knowledge was the least proficient component of digital literacy, whereas online shopping and financial operations were the most proficient.

Mai and Tick (2021) examined the degree of cyber security awareness, knowledge, and behavior among students in general, as well as the differences between Hungary and Vietnam in particular. A series of questionnaires and 313 replies were used to collect research data in Hungary and Vietnam, across various school years and disciplines of study. The quantitative analysis was carried out using SPSS. Regardless of respondent country, the results demonstrate that all respondents lack understanding about cyber security, resulting in a low degree of cyber threat awareness. However, there are slight discrepancies in behavior between respondents in Hungary and Vietnam, which were assessed using four aspects of cyber security: virus items, password usage concerns, social engineering, and online scam issues.

Rahman et al. (2020) carried out a systematic review to investigate why it is so important that students now get instruction about the dangers of using the internet and the methods that stakeholders might employ to encourage cybersecurity education in classrooms. This study discusses many options for implementing cybersecurity education in educational institutions.

Klein et al. (2020) investigated the relationship that exists between cyber security behavior, cyber knowledge, and cyber security awareness. The student's behaviors in Slovenia and Israel, two comparable nations, were measured. The findings indicate that although

students thought they had a sufficient understanding of cyber threats, they only took a few, typically straightforward precautions to keep their devices safe. The results of the study also demonstrate that knowledge about cyber threats acts as a mediator in the relationship between protective behaviors and knowledge, but only when the information is particular to IT protection courses.

Khalid and El-Maliki (2020) evaluated the concerns that the participants had as they were organizing and creating their digital tales, as well as their experiences creating digital stories regarding cyber threats. Written reflections were used to gather data. NVivo software was then used to do a thematic analysis of the data. The results show how much the respondents appreciated their involvement in the conception, creation, and assessment of their narrative films.

2.3 Conclusion

The literature related to Cyber safety and security research shows that protecting our digital information is more important than ever. The studies reveal that cyber threats are constantly evolving, with hackers using advanced techniques like phishing and ransomware. Technology, like artificial intelligence and blockchain, is seen as crucial for defending against these threats. Human error is a big concern, so education and training are recommended to prevent mistakes that could lead to breaches. Laws and regulations play a significant role in making sure companies and organizations take cybersecurity seriously. Overall, the research emphasizes the need to work together is key to staying safe online and protecting our information.

CHAPTER 3: METHODOLOGY

3.1. Introduction

The methodology section of this study outlines the systematic approach adopted to investigate the awareness of cyber safety and security among secondary-stage students (Class IX to XII) in India. Given the rising digital exposure among this demographic, it is crucial to assess their knowledge, attitudes, and practices related to cyber safety to develop effective educational interventions and policies. This study employs a mixed-methods research design, integrating both quantitative and qualitative data collection methods to provide a comprehensive understanding of the student's awareness levels and the factors influencing them. Through a combination of structured surveys and focus group discussions, the study aims to capture a holistic view of the current state of cyber safety awareness among secondary-stage students. The following sections detail the research design, sampling strategy, data collection tools, procedures, and analytical techniques employed in this study.

3.2. Research Design

The importance of research design lies in its role in providing a structured and systematic approach to conducting a study. It outlines the methodology, including data collection and analysis techniques, ensuring that the research is valid, reliable, and well-organized. A robust research design optimizes resources, minimizes bias, and enhances the quality of data collected, leading to credible and reproducible results. It also addresses ethical considerations, such as participant consent and confidentiality, ensuring the research adheres to ethical standards. By clearly defining how data will be analyzed and reported, research design helps in drawing meaningful conclusions and making informed recommendations. Furthermore, a well-planned research design facilitates the generalization of findings to a larger population and guides future replication of the study, thereby contributing to the overall reliability and advancement of knowledge in the field.

3.2.1. Design of the Study

In the study, the investigator adopted a convenience sampling method for the survey method. It is a non-probability sampling method. This sampling method includes participants who are readily available and agree to participate in a study. The major features of this type of sampling are availability, convenience, and accessibility. This method is appropriate when the study places special emphasis upon the lack of control of certain specific variables in the survey method.

3.2.2. Variables of the Study

Variables are the factors involved in addressing the research problem, which leads to the closure of the research gap. These attributes ought to impact one another. The current study investigates secondary students' levels of awareness of cyber safety and security. Hence, the following independent and dependent variables were identified for the investigation of the study:

- **Independent Variable**

  An independent variable is a variable that has been manipulated. The independent variable is purposely manipulated during observation to determine its relationship with the dependent variable. So the demographic factors Gender, Standard, States/UTs, Type of School, Locality of the school and Medium of Instruction are considered as independent variables.

- **Dependent Variable**

  The dependent variable is the level of awareness of cyber safety and security among secondary-stage students. This variable represents the degree to which students understand and are informed about various aspects of cyber safety and security, such as recognizing cyber threats, understanding safe online practices, and knowing how to protect personal information online. This awareness can be measured through surveys, questionnaires, or assessments designed to evaluate students' knowledge and attitudes towards cyber safety and security issues.

3.2.3. Hypotheses of the Study

To undertake a meaningful analysis, the following hypotheses were proposed. There are 16 hypotheses which were clubbed under three broad hypotheses as given below:

H_1: There is no significant difference in the mean score of cyber safety and security awareness of secondary students with respect to their/ the

1. Access to Internet at home
2. Possession of personal email ID
3. Participation in ICT courses
4. Availability of digital devices at home
5. Availability of own digital devices
6. Possession of personal social media account
7. Duration of use of devices per day
8. Perception about excessive screen time

H_2: There is no significant difference in the mean score of cyber safety and security awareness of secondary students with respect to

1. Locale of the school
2. Gender of the student
3. Standard in which the students are studying
4. Type of school

H_3: There is no significant difference in the mean score of different dimensions of cyber safety and security awareness of secondary students with respect to

1. Locale of the school
2. Gender of the student
3. Standard in which the students are studying
4. Type of school

3.3 Sampling Strategy

3.3.1 Population of the Study

The population of the study refers to all the secondary school students (from IX Standard to XII standard) studying in any school, whether Government, Private or Aided school, from all 28 - States and 8 Union Territories in India. There are 6.7 crore students enrolled in secondary education in the 2021-22 session (MoE, 2021). Furthermore, every student who uses the internet in accordance with the eligibility conditions.

3.3.2 Sampling Technique

The process of choosing a small group from a vast population to serve as the actual representation of that population is known as sampling. In the context of a large and geographically dispersed population, a more complex technique known as multistage sampling is employed. The multistage sampling is a complex form of cluster sampling in which the selection of samples is carried out in multiple stages (Cochran, 1977). At each stage, the population is divided into clusters or groups, and a random sample of these clusters is selected. Within each selected cluster, further sampling is done to select smaller units, and this process is repeated as necessary.

Given the vast geographical size and diversity of the population, the documented report utilized a four-phase sampling process to create the final sample for the investigation. In the first phase, the sample encompassed the entire population across all 28 states and 8 Union Territories (UTs). In the second phase, the sample included the entire population across all school boards. The third phase focused on categorizing data by school type, covering private, government, and aided schools, and including their entire student populations. In the fourth phase, the sample included all students from grades IX to XII across the schools. Only students who were using the Internet were included in the final sample for this study.
The sample was collected in four phases:

Phase 1: Selection of States and Union Territories

The first phase involved choosing every single person living in all 28 states and 8 Union Territories (UTs) in India, all 36 entities were taken. Ensuring geographic coverage and variety, this phase captured the whole range of regional variances and traits.

Table 3.1

States/UTs	Selected	Remarks
36	36	Entire Population was taken

Phase 2: Selection of School Boards

In the second phase, every student in every state and UT across all approved school boards was included in the sample. This stage was essential to creating a thorough depiction of the educational environment by incorporating the various curricula and educational systems.

Phase 3: Selection of School Type

The third phase involved selecting the entire population of students from all demographic groups attending various school kinds, such as government, private, and aided. This classification made sure that varied school settings were included, which reflected the various financial and administrative systems found in the educational system.

Phase 4: Selection of Student Selection

In the fourth phase, all students across all the schools in grades IX through XII were included in the sample wherein purposive sampling was used as only the students using the Internet were included as the sample of this study.

Table 3.2

Students	Selected	Remarks
Students of standard IX, X, XI and XII	Students of standard IX, X, XI and XII	Entire Population was taken

3.3.3 Sample Size

The sample coverage was 1,15,632 secondary school students (from IX Standard to XII) studying in any school, whether Government, Private, or Aided school, from all 28 Indian States and 8 Union Territories.

Table 3.3 Gender-wise sample distribution

S. No.	Gender	Sample
1	Male	53,929
2	Female	61,482
3	Transgender	219

Table 3.4 Standard-wise sample distribution

S. No.	Standard	Sample
1	9th Standard	38,308
2	10th Standard	38,096
3	11th Standard	5450
4	12th Standard	33,776

Table 3.5 State/ UT/ Autonomous Organization wise sample distribution

	S. No.	State/ UT/ Autonomous Organization	Sample
State/ UT	1	Andaman & Nicobar Islands	173
	2	Andhra Pradesh	1461
	3	Arunachal Pradesh	241
	4	Assam	2258
	5	Bihar	1445
	6	Chandigarh	3968
	7	Chhattisgarh	1428
	8	Dadra and Nagar Haveli & Daman and Diu	34
	9	Delhi	17360
	10	Goa	3138
	11	Gujarat	34
	12	Haryana	1720
	13	Himachal Pradesh	3518
	14	Jammu & Kashmir	1448
	15	Jharkhand	2639
	16	Karnataka	1238
	17	Kerala	3247
	18	Ladakh	12
	19	Lakshadweep	6
	20	Madhya Pradesh	2855
	21	Maharashtra	3749
	22	Manipur	164
	23	Meghalaya	96
	24	Mizoram	5350
	25	Nagaland	1967
	26	Odisha	2114

	27	Puducherry	7
	28	Punjab	13625
	29	Rajasthan	1050
	30	Sikkim	20
	31	Tamil Nadu	815
	32	Telangana	1770
	33	Tripura	114
	34	Uttar Pradesh	4580
	35	Uttarakhand	2131
	36	West Bengal	3696

Table 3.6 Type of school-wise Sample distribution

S. No.	Type of School	Sample
1	Government School	97,028
2	Aided School	6518
3	Private School	12,084

Table 3.7 Locality of School-wise Sample Distribution

S. No.	Locality of the School	Sample
1	Rural	36,467
2	Urban	79,163

Table 3.8 Medium of Instruction-wise Sample Distribution

S. No.	Medium of Instruction	Sample
1	English	90,324
2	Hindi	18,526
3	Others	6782

3.3.4 Access and Permission

The research project has been approved by the PAC of National Council of Educational Research and Training, New Delhi. Access and permission were obtained from school heads. The consent of respondents was obtained through consent guidelines via the online survey. This research aimed to gather valuable insights into students' awareness and practices regarding online safety.

3.4 Research Tool

It was determined to employ an online survey for data collection because of the unique nature of the study, as rating scales are thought to be an effective technique for gathering data in descriptive research (Lobe, Simoes, & Zaman 2009). When collecting information from a large sample, a rating scale is a more practical and effective method (Coolican, 2004; Quinn, 2013).

Due to the unique nature of this research project, it was hard to find the appropriate rating scale; a rating scale was created in order to gather relevant information from the population.

The study used an online survey method with a quantitative design; therefore, creating a tool to collect the required data was unavoidable. The research team examined a wide range of relevant literature in order to construct the tool "Cyber Safety and Security Awareness Scale (CSSAS) for Secondary Students," including country reports, peer-reviewed research articles from India and abroad, cyber safety and security guidelines for students from various national and international agencies, policy documents from India and abroad, expert opinions, etc. Dimensions were determined, and the five-point awareness was developed. The scale has five dimensions: Psychological, Physical, Legal, Socio-ethical, and Technical. Each dimension has items categorized as Strongly Agree, Agree, Undecided, Disagree and Strongly Disagree.

3.4.1 Identification of Dimensions

A five-point rating scale/ awareness tool with five dimensions on cyber safety and security was constructed, validated, and reliability was achieved by going through pilot testing. A Google form was created in English language and translated into Hindi also for the collection of data and the link was shared with all the 36 states and UTs of India for the purpose of collecting data from secondary school students for the study. Five dimensions of the rating scale are shown below:

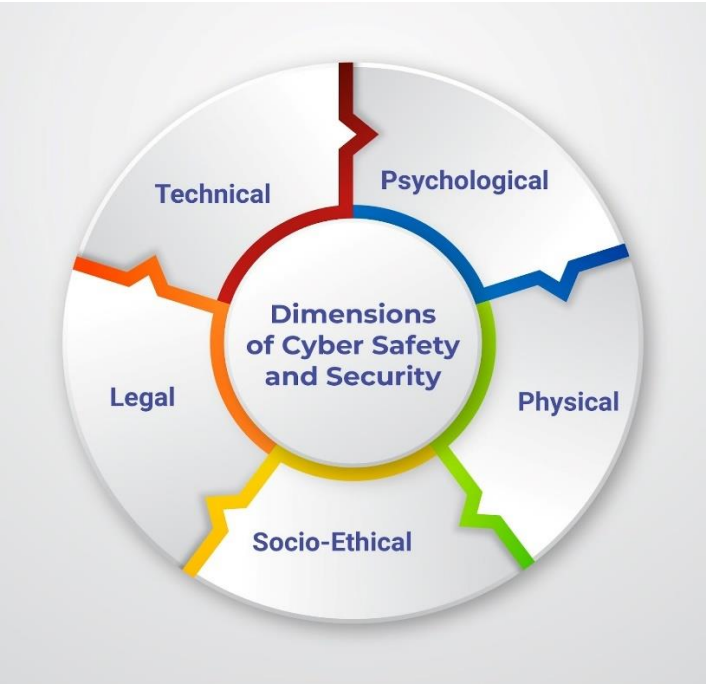


Figure 3.1: Dimension coverage

The awareness scale consists of 5 dimensions with 58 items with the 5 responses, namely; strongly agree/agree/ undecided/ disagree/ strongly disagree. Each dimension consists of items with true or false connotations with respect to cyber safety and security. The following table presents dimension-wise items with true/ false connotations.

Table 3.9: Items coverage- Dimension wise

Dimension	True	False	Total
Psychological	12	0	12
Physical	8	3	11
Legal	5	5	10
Socio-ethical	6	7	13
Technical	6	6	12
Total	**37**	**21**	**58**

3.4.2 Identification of Parameters and Attributes

Selection and Compilation of Items. Initially, a Focused Group Discussion was organized on the following questions:

1. Due to the use of digital devices, what changes do you see in lifestyle and behavioral patterns?
2. Who do you think is more appropriate to approach when you come across cyber-related problems? Teacher, Counselor? Psychologist and Why?
3. How will you handle it if you and your friends are cyberbullied?
4. How do you protect your digital device? Explain.
5. What precautions do you take when you access public WIFI?
6. What information will you share publicly or on social media platforms?

In this Focused Group Discussion, five dimensions of the rating scale were finalized. 120 items were developed through a rigorous review of literature available on different websites, previous studies were also considered for selecting items. After the discussion with experts, 100 items were found suitable, and these 100 items were divided into five parts:

Table 3.10

Dimension	Parameter	Indicator	Example
Technical	Device Safety	Antivirus installation	
		Installation from authentic Software/apps	
		Piracy	
		Updation of the device software	

		Password protection	
		Authorization and authentication for external devices	
		Accessing wireless devices and WIFI connections	
		Managing apps and software	
	Data Safety	Accessing information from anonymous/unauthorized sources	suspicious links, unauthorized links, HTTPS
		Data Backup	
		Data protection	OTP and passwords
		Privacy settings	setting filters
Social and Ethical	Confidentiality	Accessing and Sharing information without consent	Accessing another email, and passwords, signing out devices with not in use, misusing information, taking parents' consent/permission
		Leaving Device/application/Data unattended	
	Identity	Creating/Accessing/Sharing Fake Profiles/ Documents	
		Accessing and Sharing the personal information	Footprints
	Accuracy/ Information literacy	verifying information	misinformation, fake news, profile
	Intellectual Property & Copyright	Plagiarism	Credits of information, Copying information without consent
Legal	Identifying Cyber Crime	Intellectual Property Crime/ Copyright	
		Cyber Stalking/harassment	
		Financial	
		Derogatory comments	

	Cyber law	Cyber pornography	Legal offense for using child pornography
		Copyright	
		hacking	
		Violation of Privacy	Data breach and misuse of information
		Creation and sharing of misinformation	
	Reporting	Various forms of reporting	Helpline, police station, complaint box, Principal, Parents/ Guardians
		Essentials for reporting	Forms of evidence
Physical	Ergonomics	Posture	neck, back, arm, finger, hand, wrist and elbow pain, body posture, body positioning
		Positioning of gadgets and furniture	
	Impact/Consequences	Eye strain	
		Hearing Loss	
		Accidents	
		radiations	
		Obesity	
Psychological	Consequences	Sleep disruption	
		Span of attention	
		Isolation	
		Addiction	
		Anxiety and Fear	
		self-image	
		Depression	
	Support system	Counselors	
		Helpline	
		Clinics	

3.4.3 Development of Items

As cited above there was a Multiple choice scale used in this study. A brief description of the Multiple choice scale' development is presented in the following heads- Scale for Students:

Structure of Rating Scale, Blueprint of Students' Rating Scale

Table 3.11

Purpose of the Rating Scale	A Study of the Awareness on Cyber Safety and Security Among Secondary Students (Class IX to XII)
Nature of the Rating Scale	Unstructured, Close Ended
Parts	Three or four
Sections	Personal Information General Information Rating Scale
Dimensions	Psychological 12
	Physical 11
	Legal 10
	Socio-ethical 13
	Technical 12
Total number of items	58

3.4.4 Development of the Research Tool

One of the objectives of the research was to develop a research tool to measure the level of cyber safety and security awareness among students. In the research process, a workshop was conducted to gather expert input, which was then complemented by a thorough analysis and review of existing literature. This combined approach was utilized to identify and define the primary dimensions for the development of the measurement scale. pon identifying the dimensions, parameters and sub-parameters were defined under each dimension. Further, for tool development, individual items were designed under each dimension covering all the parameters. The research tool developed by CIET-NCERT is termed "The Cyber Safety And Security Awareness Scale".

A series of workshops were also conducted at CIET-NCERT to review the scale from external experts.

Workshop 1: To review the Tool Developed

A Three days workshop was conducted to review the questionnaire developed with the following objectives:

- To review the cyber safety and security awareness research tools developed for students.
- To finalize the cyber safety and security awareness research tools developed for students.

The workshop was conducted in the blended mode where resource persons were given an option to join the workshop in face-to-face mode from CIET-NCERT whereas outstation resource persons from ISEA-CDAC had an option to join the workshop online and review the parameters and items developed to assess the level of cyber safety awareness among various stakeholders. At the end of this workshop, all the items of the tool were reviewed and the tool was finalized. The finalized research tool developed which is termed as "Cyber Safety And Security Awareness Scale" consists of 58 items, each part consisting of 5 dimensions namely, technical aspects, legal aspects, social-ethical aspects and physical-psychological aspects. These 5 dimensions cover 16 parameters and 25 sub-parameters. The developed questionnaire is attached as Annexure I.

3.4.5 Pilot of Research Tool

A feasibility study, sometimes called a pilot study, is a small-scale investigation carried out before a more extensive, full-scale investigation. It serves as a trial run to evaluate the viability, usefulness, and efficacy of the techniques and protocols intended for the primary study. A pilot study was done on a small sample of secondary students. A sample of 302 secondary students was chosen, and the research tool was administered to them to establish the reliability, viability, usefulness, and efficacy of the research tool.

3.4.6 Validity & Reliability

Validation of Tool: The validity and reliability of the scales employed in research are critical aspects that allow the research to provide useful results. For this reason, it is important to understand how researchers appropriately assess the scales' reliability and validity (Surucu & Maslakci, 2020). A research study may comprise only part of the methodological subspace's elements, which include scientific standards, procedures, and principles. Examples of these elements are validity systems. This subspace is utilized in substantive research to establish knowledge claims and comprises information derived from methodological research (Lund, 2022).

The literature synthesis produced themes and codes for item development in scale based on worldwide and Indian research papers, reports, and policy guidelines, as well as the identified research deficit. The expert members structured the questions and items on the background variables and dimensions of the scale using the themes and codes. The scale contains five dimensions: psychological, physical, legal, socio-ethical, and technical. Individual Items were developed using the dimensions. The items were labelled as Strongly Agree, Agree, Undecided, Disagree and Strongly Disagree. The scale has three parts which are mentioned below:

Part 1:Demographic information of respondents (Personal information).

Part 2: Information related to ICT and digital exposure of respondents (General information).

Part 3: Rating scale related to Cyber Safety and Security Awareness (CSSA).

The developed questions on the background variables and items under each dimension were then examined for face validity and content validity by the national-level experts. Based on their validity examination, some items were removed, and a few were added.

- **Face Validity:** Face validity was checked by the research team members first, and then by the Program Coordinator, 80 questions and 5 dimensions were finalized.
- **Content Validity**. The rating scale was validated by 7 experts in the field. Later, the panel of experts was formed based on expertise in psychology, sociology, law, and educational technology; a minimum of five years of experience in concerned fields was required. Three professors and four assistant professors constituted the panel of experts.

The experts' suggestions regarding objectivity, and suitability of items were taken into consideration. Language difficulty was removed by replacing difficult words with easy ones. In the final rating scale out of 80 items, 58 items were selected and reframed according to the need of the study and the rest were removed. All the suggestions given by experts were incorporated in the final tool. It is only after the validation; that the tool was administered to the sample.

To determine the flaws and limitations and to achieve reliability and validity of the rating scale, pilot testing was done on a small sample of 302 secondary school students. It enables us to refine the instrument and make necessary improvements before the final implementation. A pilot test was conducted on 130 students to ensure the accuracy of items and whether it addressed research questions or not.

Reliability of Research Tool:

Reliability refers to the consistency and stability of a measurement over repeated administrations or observations. A reliability score close to 1.0 indicates a high level of consistency, meaning that the measurement is highly dependable and yields similar results under consistent conditions. The statistical analysis was conducted using version 28.0 of the Statistical Package for the Social Sciences (SPSS). Cronbach's alpha was used to determine the CSSAS quality score's internal consistency. A reliability score of 0.9933 was derived from statistical analyses, indicating that the measurement instrument has demonstrated exceptional reliability in the context of the research study. In research, a reliability score of 0.9933 typically indicates a very high level of reliability of the tool. It also suggests that the measurement instrument or tool used in the study demonstrates an extremely high level of consistency and stability. This high-reliability score implies that the measurement is highly trustworthy and can be relied upon to produce consistent and accurate results across multiple administrations or observations.

3.4.7 Finalisation of Tool

After the pilot study, a few more modifications were made to the rating scale before the final administration of the students. Here irrelevant and invalid items were removed, and at the end, 58 items were left in the final rating scale.

3.4.8 Translation of Tool

Translating a research tool is critical for guaranteeing the inclusion, precision, and validity of research. Translating a research tool makes it accessible to individuals who do not speak the original language. Translation of research tools into other languages ensures that students who do not know the original language have equal access to participate in the study; it may improve sample representativeness and generalizability.

The translation process is extensive and detailed, requiring knowledge of the subject idea, conversion, and presentation of complicated concepts in their simplest form. The population covers senior secondary students from all 28 Indian States and 8 Union Territories, and the sample was selected from that, so the translation of the awareness scale in the mother tongue was required.

3.5 Data Collection

The current study used a quantitative research design, which is empirical in nature i.e., it focuses on numbers and statistics, and is critical for revealing the educational landscape. It is effective for educators, policymakers, and researchers alike, providing crucial insights to inspire evidence-based policies and enhance learning outcomes. The study includes all 28 States and 8 Union territories in India. An online survey method was used to collect data from multiple schools, including diversity in population, school settings, languages, etc. A descriptive survey was done using Google Forms among students from secondary schools to find out their awareness on cyber safety and security based on different dimensions. Getting accurate details on an existing situation is the aim of a descriptive survey study in order to decide what should happen next (Good, 1972). An Online-based survey was used to collect the data. This was due to covering samples of all 28 Indian States and 8 Union Territories. Permission from the school authorities/ teachers was obtained, and consent was also obtained from the students for the data collection.

Time allocation was maintained for each step of the empirical investigation of this study, including project conception, literature review, tool construction, validation, pilot study, reliability attainment, primary data collection, data analysis, and report writing.

The online tool was administered in English and bilingual mode, and a Google form link of the research tool was shared with each of the 28 States and 8 Union Territories in India for fifteen days.

Procedure of Data Collection: The next step after defining the sample and instrumentation is data collection. The Google form link/ rating scale was directly sent to the states and UTs, which was further shared with the sample students. The consent of the students was taken.

3.6 Data Analysis

The quantitative data was analyzed under descriptive and inferential parameters. The items which are in the scale have five-point rating scale connotations based on the connotations with respect to cyber safety and security. Each item has 5 responses. All items that are labeled as true have responses as strongly agree, agree, undecided, disagree, and strongly disagree with scoring 5, 4, 3, 2, 1, respectively. All items that are labeled as false have responses as strongly disagree, disagree, undecided, agree, and strongly agree with scoring 1,2,3,4,5, respectively. The results were presented in tables and figures. The quantitative data was analyzed under descriptive and inferential parameters. Ms-Excel was used for Descriptive analysis, and SPSS Software for inferential analysis; t-test, ANOVA etc. were used. The result was presented in tables and figures.

3.6.1 Statistical Analysis for Quantitative Data

Statistical analysis is an essential component of quantitative research (Kee et al., 2013). Quantitative data is usually associated with numbers, and Quantitative research has the advantage of establishing a sequence of processes that allow for the standardized investigation of phenomena, thus significantly reducing the researcher's bias (Suárez et al., 2017). A popular approach for formulating and addressing quantitative research questions is to identify a gap in the current literature and conduct a study to fill it (Jamieson et al., 2023).

For the statistical analysis, data was exported to an Excel file and was cleaned. After this, the collected data which were in alpha-numeric format were coded to numerics, so as to make the analysis easier. The score of the CSSA tool was calculated dimension-wise as well as in total. The cleaned and coded data was then exported into SPSS (Version 27) for further analysis. The details of the analysis carried out along with the findings and discussion are presented in the following chapter.

3.7 Limitations of the Study

This nationwide quantitative study has its own limitations. They are limited with Age range, educational setting, Coverage of dimensions, Research method, School education, and coverage of languages in tools.

- **Age Range:** The study focused solely on students in grades 9–12, omitting younger or older age groups. This delimitation ensures a specific assessment of cyber safety and security awareness within the context of secondary school.
- **Educational Setting:** Students enrolled in government, private, and aided schools were the only subjects of the study; homeschoolers and participants in alternative education programs were not included. An investigation in a more homogeneous sample and context was made possible by this delimitation.
- **Dimensions of Cyber Safety and Security:** The study concentrated only on five dimensions of cyber safety and security that are pertinent to students in grades 9 through 12, including Psychological, Physical, Legal, Socio-ethical and Technical. This boundary guarantees a targeted analysis of the most important cyber safety and security concerns that affect the intended sample.

- **Research Method:** The study adopted online surveys through Google Forms and quantitative analysis.
- **Language coverage:** The tool of the study was prepared in English and Hindi.

The results and interpretation along with its discussion will be presented in the next chapter.

CHAPTER 4: RESULTS AND INTERPRETATION

4.1. Introduction

Data analysis is the systematic procedure of applying logical and statistical methods for describing, illustrating, condensing and assessing the research data. According to Creswell (2002), qualitative research is a strategy for data collection, analysis, and report writing that is distinct from the conventional, quantitative approaches. Quantitative research is the process of gathering, analyzing, interpreting, and producing study results.

4.2 Data Analysis and Interpretation

Analyzing and interpreting data entails systematically going over gathered information to find trends, connections, and revelations that help with decision-making. This procedure entails cleaning and arranging the data, analyzing it using statistical or computational techniques, and producing a meaningful summary of the results. Interpretation is more than just summarizing the findings; it also entails placing the data in the larger context of the study question or issue, coming to conclusions, and drawing conclusions from the analysis.

4.2.1 Nature of Distribution of Samples Across Subgroups

In this primary section, the distribution of selected samples across the subgroups is provided across different states. This has been done to have a better insight about the sample distribution

4.2.1.1: State-wise distribution of sample with regard to Gender

Table 4.1 State-wise distribution of sample with regard to Gender

State / Union Territory	Gender	Response (Number)	Response (Percentage)
Andaman and Nicobar Islands	Female	87	50.3
	Male	79	45.7
	Transgender	7	4
	Total	173	100
Andhra Pradesh	Female	785	53.7
	Male	673	46.1
	Transgender	3	0.2
	Total	1461	100
Arunachal Pradesh	Female	121	50.2
	Male	119	49.4

	Transgender	1	0.4
	Total	241	100
Assam	Female	1148	50.8
	Male	1106	49
	Transgender	4	0.2
	Total	2258	100
Bihar	Female	614	42.5
	Male	826	57.2
	Transgender	5	0.3
	Total	1445	100
Chandigarh	Female	1990	50.2
	Male	1960	49.4
	Transgender	18	0.5
	Total	3968	100
Chhattisgarh	Female	722	50.6
	Male	704	49.3
	Transgender	2	0.1
	Total	1428	100
Dadra and Nagar Haveli and Daman and Diu	Female	14	41.2
	Male	17	50
	Transgender	3	8.8
	Total	34	100
Delhi	Female	24523	56.8
	Male	18612	43.1
	Transgender	73	0.2
	Total	43208	100
Goa	Female	1998	57.9
	Male	1450	42

	Transgender	1	0
	Total	3449	100
Gujarat	Female	15	44.1
	Male	18	52.9
	Transgender	1	2.9
	Total	34	100
Haryana	Female	762	44.3
	Male	952	55.3
	Transgender	6	0.3
	Total	1720	100
Himachal Pradesh	Female	1816	51.6
	Male	1701	48.4
	Transgender	1	0
	Total	3518	100
Jammu & Kashmir	Female	740	51.1
	Male	708	48.9
	Total	1448	100
Jharkhand	Female	1235	46.8
	Male	1402	53.1
	Transgender	2	0.1
	Total	2639	100
Karnataka	Female	623	50.3
	Male	615	49.7
	Total	1238	100
Kerala	Female	1719	52.9
	Male	1527	47
	Transgender	1	0
	Total	3247	100

Ladakh	Female	1	8.3
	Male	10	83.3
	Transgender	1	8.3
	Total	12	100
Lakshadweep	Female	4	66.7
	Male	2	33.3
	Total	6	100
Madhya Pradesh	Female	1354	47.4
	Male	1498	52.5
	Transgender	3	0.1
	Total	2855	100
Maharashtra	Female	1744	46.5
	Male	2003	53.4
	Transgender	2	0.1
	Total	3749	100
Manipur	Female	94	57.3
	Male	70	42.7
	Total	164	100
Meghalaya	Female	41	42.7
	Male	55	57.3
	Total	96	100
Mizoram	Female	2929	54.7
	Male	2419	45.2
	Transgender	2	0
	Total	5350	100
Nagaland	Female	1062	54
	Male	903	45.9
	Transgender	2	0.1

	Total	1967	100
Odisha	Female	1027	48.6
	Male	1086	51.4
	Transgender	1	0
	Total	2114	100
Puducherry	Female	4	57.1
	Male	3	42.9
	Total	7	100
Punjab	Female	7514	55.1
	Male	6043	44.4
	Transgender	68	0.5
	Total	13625	100
Rajasthan	Female	477	45.4
	Male	571	54.4
	Transgender	2	0.2
	Total	1050	100
Sikkim	Female	13	65
	Male	7	35
	Total	20	100
Tamil Nadu	Female	424	52
	Male	391	48
	Total	815	100
Telangana	Female	917	51.8
	Male	852	48.1
	Transgender	1	0.1
	Total	1770	100
Tripura	Female	53	46.5
	Male	60	52.6

	Transgender	1	0.9
	Total	114	100
Uttar Pradesh	Female	2098	45.8
	Male	2475	54
	Transgender	7	0.2
	Total	4580	100
Uttarakhand	Female	1035	48.6
	Male	1096	51.4
	Total	2131	100
West Bengal	Female	1779	48.1
	Male	1916	51.8
	Transgender	1	0
	Total	3696	100

From above table 4.1, the distribution of data is based on the state wise with regard to gender. There are 21 states and UTs in which the Female has the highest number. In Delhi, females are the most populous gender group, comprising 24,523 individuals, which accounts for 56.8% of the total population of 43,208. This indicates that there are more females than males in the population of Delhi. In 15 states and UTs, Males have the highest number. In Uttar Pradesh (UP), males form the predominant gender group, totalling 2,475 individuals, which accounts for 54% of the state's total population of 4,580. This demographic composition highlights a significant male majority within the region. There are significantly more males than females based on the given data in UP. In Chandigarh, transgender individuals account for 18 persons, making up 0.5% of the total population of 3,968. It indicates their numerical representation as a minority within the broader population.

The distribution is graphically represented in the following figures (fig 4.1, 4.2, 4.3)

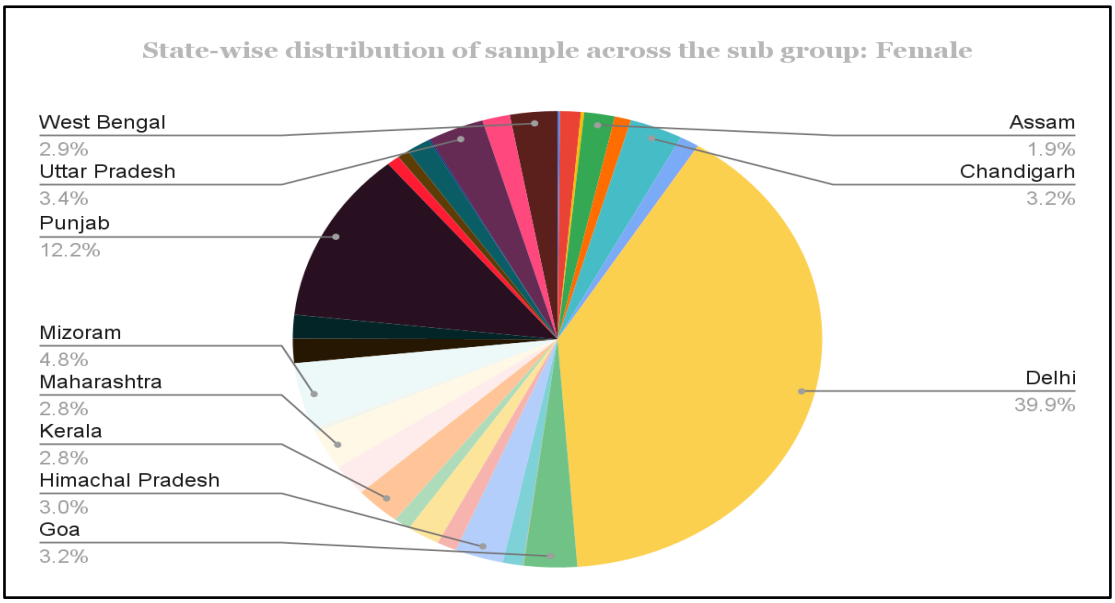


Fig 4.1: State-wise distribution of sample across the sub-group: Female

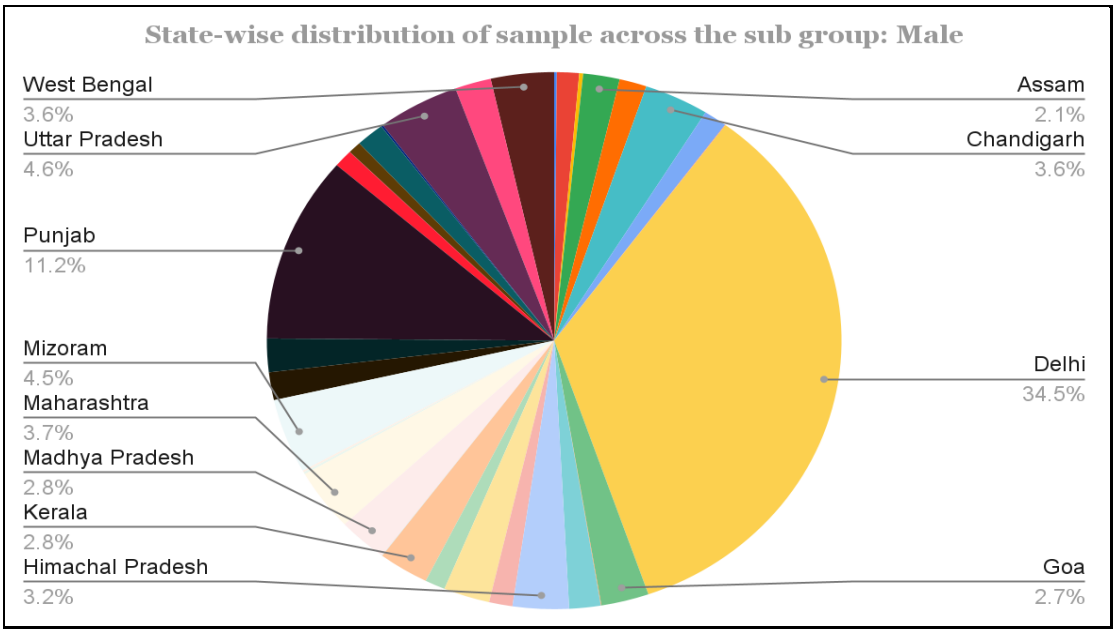


Fig 4.2: State-wise distribution of sample across the sub-group: Male

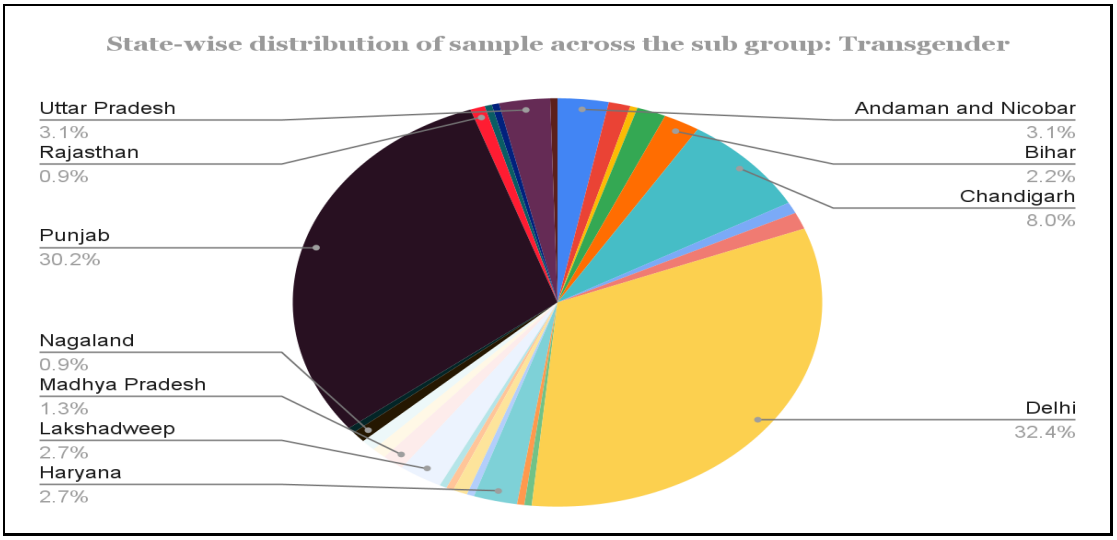


Fig 4.3: State-wise distribution of sample across the sub group: Transgender

It is evident from the above section that the majority of students were from Punjab, Delhi and Chandigarh irrespective of their gender.

4.2.1.2: State-wise distribution of sample with regard to Standard

Table 4.2: State-wise distribution of sample with regard to Standard

State / Union Territory	Standard	Response (Number)	Response (Percentage)
Andaman and Nicobar Islands	10th Standard	62	35.8
	11th Standard	7	4.0
	12th Standard	18	10.4
	9th Standard	86	49.7
	Total	173	100.0
Andhra Pradesh	10th Standard	662	45.3
	11th Standard	24	1.6
	12th Standard	252	17.2
	9th Standard	523	35.8
	Total	1461	100.0
Arunachal Pradesh	10th Standard	101	41.9
	11th Standard	3	1.2
	12th Standard	59	24.5
	9th Standard	78	32.4
	Total	241	100.0
Assam	10th Standard	813	36.0
	11th Standard	48	2.1
	12th Standard	558	24.7
	9th Standard	839	37.2
	Total	2258	100.0

Bihar	10th Standard	505	34.9
	11th Standard	68	4.7
	12th Standard	359	24.8
	9th Standard	513	35.5
	Total	1445	100.0
Chandigarh	10th Standard	1179	29.7
	11th Standard	227	5.7
	12th Standard	1203	30.3
	9th Standard	1359	34.2
	Total	3968	100.0
Chhattisgarh	10th Standard	497	34.8
	11th Standard	33	2.3
	12th Standard	445	31.2
	9th Standard	453	31.7
	Total	1428	100.0
Dadra and Nagar Haveli and Daman and Diu	10th Standard	11	32.4
	11th Standard	5	14.7
	12th Standard	4	11.8
	9th Standard	14	41.2
	Total	34	100.0
Delhi	10th Standard	13762	31.9
	11th Standard	1342	3.1
	12th Standard	1	.0
	9th Standard	14911	34.5
	Total	13192	30.5
	10th Standard	43208	100.0
Goa	10th Standard	1253	36.3
	11th Standard	271	7.9
	12th Standard	934	27.1
	9th Standard	991	28.7
	Total	3449	100.0
Gujarat	10th Standard	8	23.5
	11th Standard	4	11.8
	12th Standard	8	23.5
	9th Standard	14	41.2
	Total	34	100.0
Haryana	10th Standard	462	26.9
	11th Standard	71	4.1
	12th Standard	580	33.7
	9th Standard	607	35.3
	Total	1720	100.0
Himachal Pradesh	10th Standard	967	27.5

	11th Standard	528	15.0
	12th Standard	980	27.9
	9th Standard	1043	29.6
	Total	3518	100.0
Jammu & Kashmir	10th Standard	473	32.7
	11th Standard	221	15.3
	12th Standard	360	24.9
	9th Standard	394	27.2
	Total	1448	100.0
Jharkhand	10th Standard	920	34.9
	11th Standard	18	.7
	12th Standard	619	23.5
	9th Standard	1082	41.0
	Total	2639	100.0
Karnataka	10th Standard	514	41.5
	11th Standard	20	1.6
	12th Standard	190	15.3
	9th Standard	514	41.5
	Total	1238	100.0
Kerala	10th Standard	1153	35.5
	11th Standard	35	1.1
	12th Standard	776	23.9
	9th Standard	1283	39.5
	Total	3247	100.0
Ladakh	10th Standard	5	41.7
	11th Standard	1	8.3
	12th Standard	1	8.3
	9th Standard	5	41.7
	Total	12	100.0
Lakshadweep	10th Standard	4	66.7
	9th Standard	2	33.3
	Total	6	100.0
Madhya Pradesh	10th Standard	976	34.2
	11th Standard	18	.6
	12th Standard	598	20.9
	9th Standard	1263	44.2
	Total	2855	100.0
Maharashtra	10th Standard	1443	38.5
	11th Standard	54	1.4
	12th Standard	857	22.9
	9th Standard	1395	37.2
	Total	3749	100.0

Manipur	10th Standard	53	32.3
	12th Standard	52	31.7
	9th Standard	59	36.0
	Total	164	100.0
Meghalaya	10th Standard	33	34.4
	12th Standard	29	30.2
	9th Standard	34	35.4
	Total	96	100.0
Mizoram	10th Standard	1681	31.4
	11th Standard	25	.5
	12th Standard	1696	31.7
	9th Standard	1948	36.4
	Total	5350	100.0
Nagaland	10th Standard	599	30.5
	11th Standard	36	1.8
	12th Standard	643	32.7
	9th Standard	689	35.0
	Total	1967	100.0
Odisha	10th Standard	733	34.7
	11th Standard	33	1.6
	12th Standard	510	24.1
	9th Standard	838	39.6
	Total	2114	100.0
Puducherry	10th Standard	4	57.1
	12th Standard	1	14.3
	9th Standard	2	28.6
	Total	7	100.0
Punjab	10th Standard	4370	32.1
	11th Standard	1999	14.7
	12th Standard	3414	25.1
	9th Standard	3842	28.2
	Total	13625	100.0
Rajasthan	10th Standard	318	30.3
	11th Standard	20	1.9
	12th Standard	286	27.2
	9th Standard	426	40.6
	Total	1050	100.0
Sikkim	10th Standard	1	5.0
	11th Standard	1	5.0
	12th Standard	15	75.0
	9th Standard	3	15.0
	Total	20	100.0

Tamil Nadu	10th Standard	284	34.8
	11th Standard	13	1.6
	12th Standard	150	18.4
	9th Standard	368	45.2
	Total	815	100.0
Telangana	10th Standard	807	45.6
	11th Standard	10	.6
	12th Standard	238	13.4
	9th Standard	715	40.4
	Total	1770	100.0
Tripura	10th Standard	41	36.0
	11th Standard	3	2.6
	12th Standard	44	38.6
	9th Standard	26	22.8
	Total	114	100.0
Uttar Pradesh	10th Standard	1595	34.8
	11th Standard	185	4.0
	12th Standard	1206	26.3
	9th Standard	1594	34.8
	Total	4580	100.0
Uttarakhand	10th Standard	644	30.2
	11th Standard	28	1.3
	12th Standard	654	30.7
	9th Standard	805	37.8
	Total	2131	100.0
West Bengal	10th Standard	1163	31.5
	11th Standard	98	2.7
	12th Standard	1126	30.5
	9th Standard	1309	35.4
	Total	3696	100.0

From the above table 4.2, the data was distributed state-wise with regard to their standard. The state-wise data for the 10th standard shows varying numbers of students enrolled, with states like Delhi (13,762), Punjab (4370), Maharashtra (1,443), and Uttar Pradesh (1,595) having relatively higher figures, while smaller states like Sikkim (1) and Dadra and Nagar Haveli and Daman and Diu (11) have lower enrollments. States like Delhi and Punjab have notably high enrollments in the 11th standard. In Punjab, the enrollment in the 11th standard is substantial, with a total of 1,999 students, which represents 14.7% of the total student population across different standards in the state. In Delhi, the enrollment in the 11th standard is also notable, with 1,342 students, constituting 3.1% of the total student population across different standards in the region. Whereas states like Gujarat and Sikkim have much lower enrollments in comparison.

Among the states and union territories listed, Mizoram stands out with the highest enrollment in the 12th standard, totaling 1,696 students, which represents 31.7% of its total student population across different standards. This indicates a significant focus on higher secondary education in Mizoram compared to other regions.

Among the states and union territories listed, Delhi has the highest enrollment in the 9th standard, with 14,911 students, accounting for 34.5% of its total student population across different standards. This highlights a substantial emphasis on secondary education at the 9th standard level in Delhi compared to other regions.

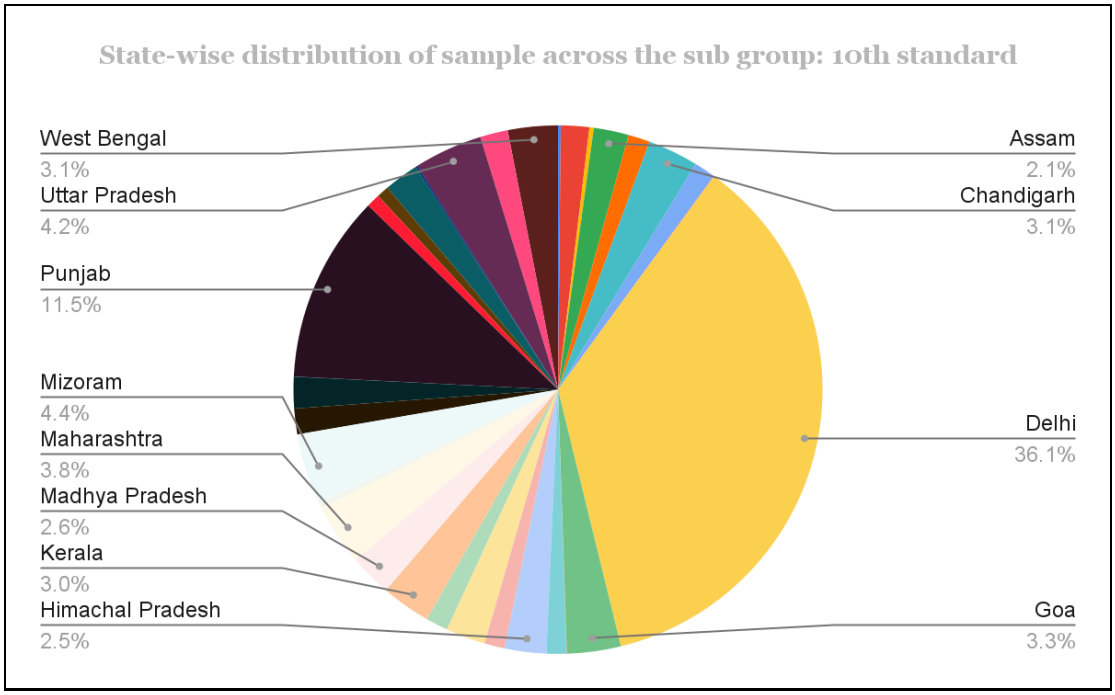


Fig 4.4: State-wise distribution of sample across the sub group: 10th standard

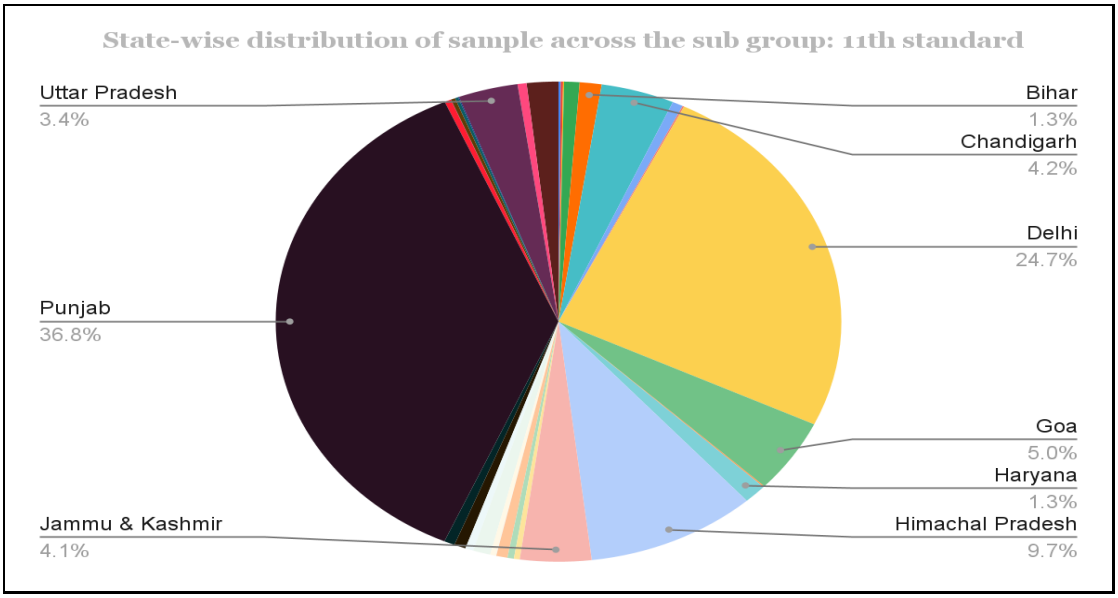


Fig 4.5: State-wise distribution of sample across the sub group: 11th standard

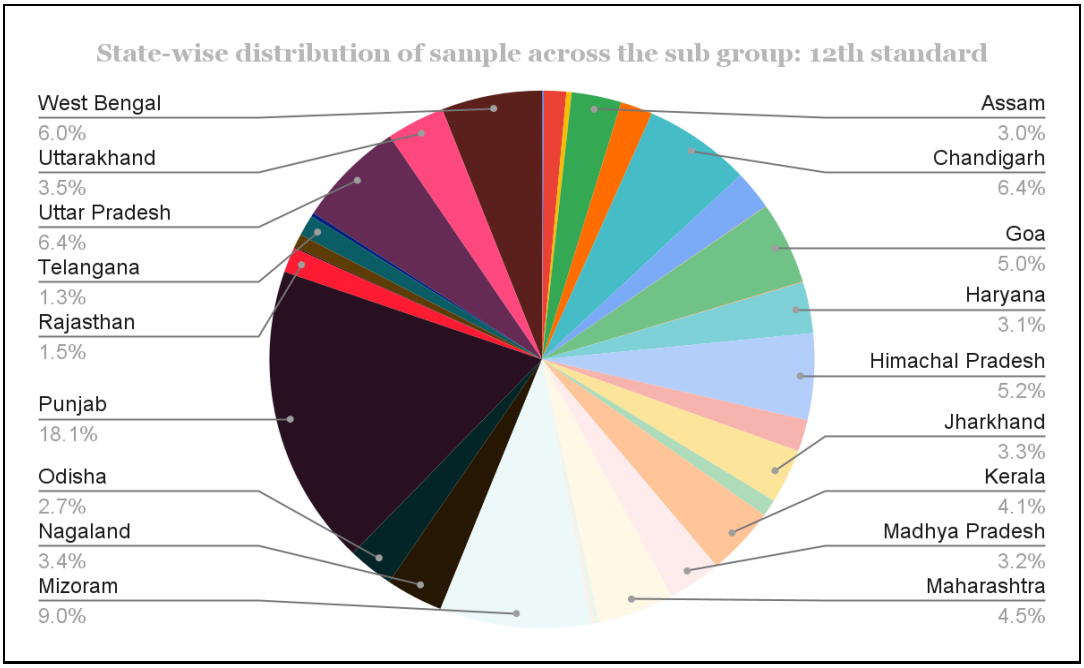


Fig 4.6: State-wise distribution of sample across the sub group: 12th standard

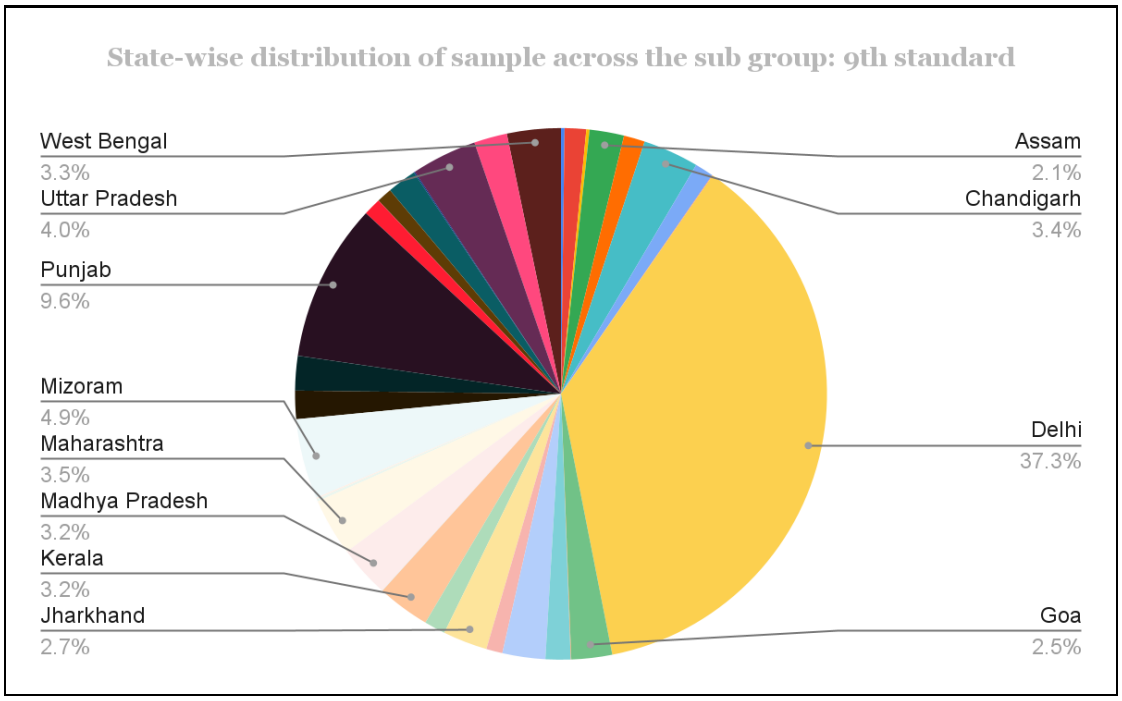


Fig 4.7: State-wise distribution of sample across the sub group: 9th standard

From the above section, it is clear that a major share of 12th standard students participated in the survey are from Punjab and mizoram. Whereas maximum participation of students of other standards are from Punjab and Delhi.

4.2.1.3: State-wise Distribution of Sample with regard to Type of School

Table 4.3: State-wise Distribution of sample with regard to Type of School

State / Union Territory	Type of School	Response (Number)	Response (Percentage)
Andaman and Nicobar Islands	Aided	18	10.4
	Government	146	84.4
	Private	9	5.2
	Total	173	100.0
Andhra Pradesh	Aided	150	10.3
	Government	1208	82.7
	Private	103	7.0
	Total	1461	100.0
Arunachal Pradesh	Aided	44	18.3
	Government	181	75.1
	Private	16	6.6
	Total	241	100.0
Assam	Aided	73	3.2
	Government	2112	93.5
	Private	73	3.2
	Total	2258	100.0
Bihar	Aided	95	6.6
	Government	1287	89.1
	Private	63	4.4
	Total	1445	100.0
Chandigarh	Aided	92	2.3
	Government	2556	64.4
	Private	1320	33.3
	Total	3968	100.0
Chhattisgarh	Aided	68	4.8
	Government	1306	91.5
	Private	54	3.8
	Total	1428	100.0
Dadra and Nagar Haveli and Daman and Diu	Aided	3	8.8
	Government	26	76.5
	Private	5	14.7
	Total	34	100.0
Delhi	Aided	2265	5.2
	Government	38005	88.0
	Private	2938	6.8
	Total	43208	100.0
Goa	Aided	931	27.0
	Government	1642	47.6

	Private	876	25.4
	Total	3449	100.0
Gujarat	Aided	4	11.8
	Government	29	85.3
	Private	1	2.9
	Total	34	100.0
Haryana	Aided	114	6.6
	Government	1413	82.2
	Private	193	11.2
	Total	1720	100.0
Himachal Pradesh	Aided	127	3.6
	Government	2495	70.9
	Private	896	25.5
	Total	3518	100.0
Jammu & Kashmir	Aided	96	6.6
	Government	1241	85.7
	Private	111	7.7
	Total	1448	100.0
Jharkhand	Aided	154	5.8
	Government	2379	90.1
	Private	106	4.0
	Total	2639	100.0
Karnataka	Aided	76	6.1
	Government	1106	89.3
	Private	56	4.5
	Total	1238	100.0
Kerala	Aided	149	4.6
	Government	2997	92.3
	Private	101	3.1
	Total	3247	100.0
Ladakh	Government	11	91.7
	Private	1	8.3
	Total	12	100.0
Lakshadweep	Aided	1	16.7
	Government	3	50.0
	Private	2	33.3
	Total	6	100.0
Madhya Pradesh	Aided	107	3.7
	Government	2718	95.2
	Private	30	1.1
	Total	2855	100.0
Maharashtra	Aided	109	2.9
	Government	3345	89.2

	Private	295	7.9
	Total	3749	100.0
Manipur	Aided	5	3.0
	Government	152	92.7
	Private	7	4.3
	Total	164	100.0
Meghalaya	Aided	9	9.4
	Government	84	87.5
	Private	3	3.1
	Total	96	100.0
Mizoram	Aided	849	15.9
	Government	3659	68.4
	Private	842	15.7
	Total	5350	100.0
Nagaland	Aided	96	4.9
	Government	238	12.1
	Private	1633	83.0
	Total	1967	100.0
Odisha	Aided	65	3.1
	Government	2025	95.8
	Private	24	1.1
	Total	2114	100.0
Puducherry	Aided	2	28.6
	Government	5	71.4
	Total	7	100.0
Punjab	Aided	362	2.7
	Government	11208	82.3
	Private	2055	15.1
	Total	13625	100.0
Rajasthan	Aided	55	5.2
	Government	957	91.1
	Private	38	3.6
	Total	1050	100.0
Sikkim	Aided	3	15.0
	Government	16	80.0
	Private	1	5.0
	Total	20	100.0
Tamil Nadu	Aided	52	6.4
	Government	731	89.7
	Private	32	3.9
	Total	815	100.0
Telangana	Aided	153	8.6
	Government	1545	87.3

	Private	72	4.1
	Total	1770	100.0
Tripura	Aided	9	7.9
	Government	104	91.2
	Private	1	.9
	Total	114	100.0
Uttar Pradesh	Aided	62	1.4
	Government	4471	97.6
	Private	47	1.0
	Total	4580	100.0
Uttarakhand	Aided	58	2.7
	Government	2048	96.1
	Private	25	1.2
	Total	2131	100.0
West Bengal	Aided	62	1.7
	Government	3579	96.8
	Private	55	1.5
	Total	3696	100.0

The above table 4.3, the result shows that Delhi stands out with the highest percentage of government schools at 88.0%. Punjab has the highest percentage in aided schools at 2.7%, and Goa has the highest percentage in private schools at 25.4%.

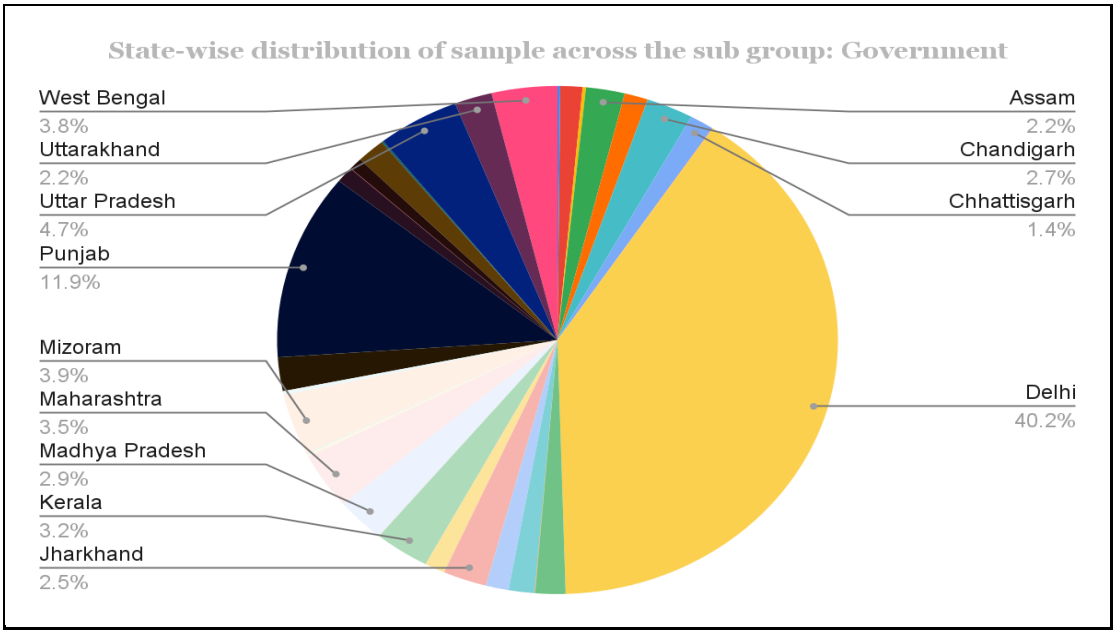


Fig 4.8: State-wise distribution of sample across the sub group: Government

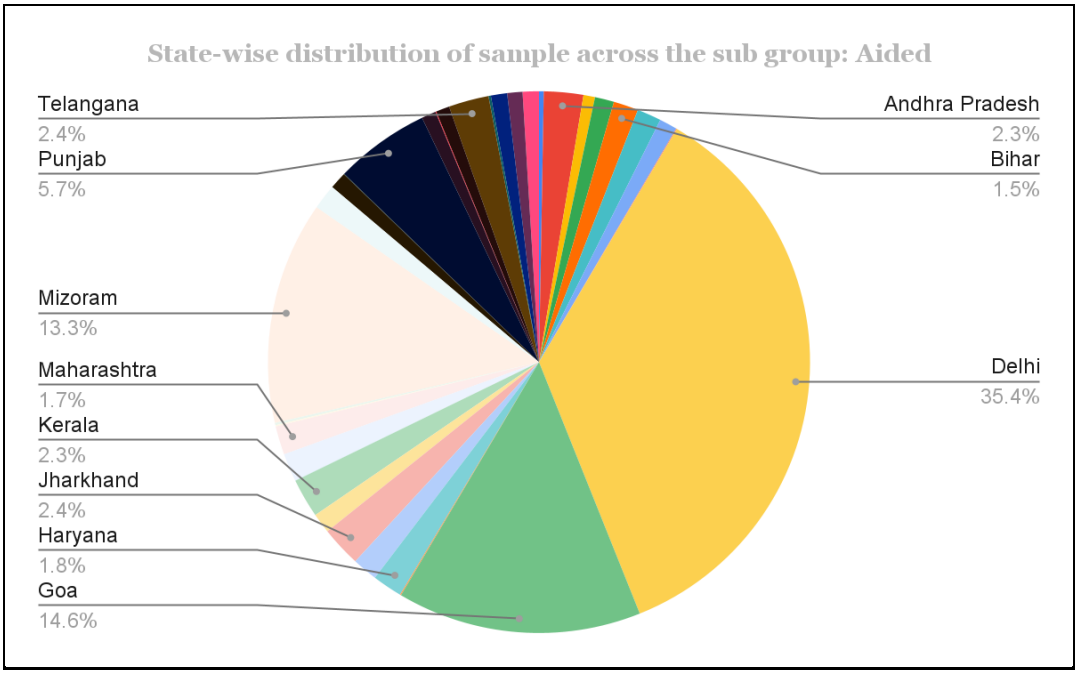


Fig 4.9: State-wise distribution of sample across the sub group: Aided

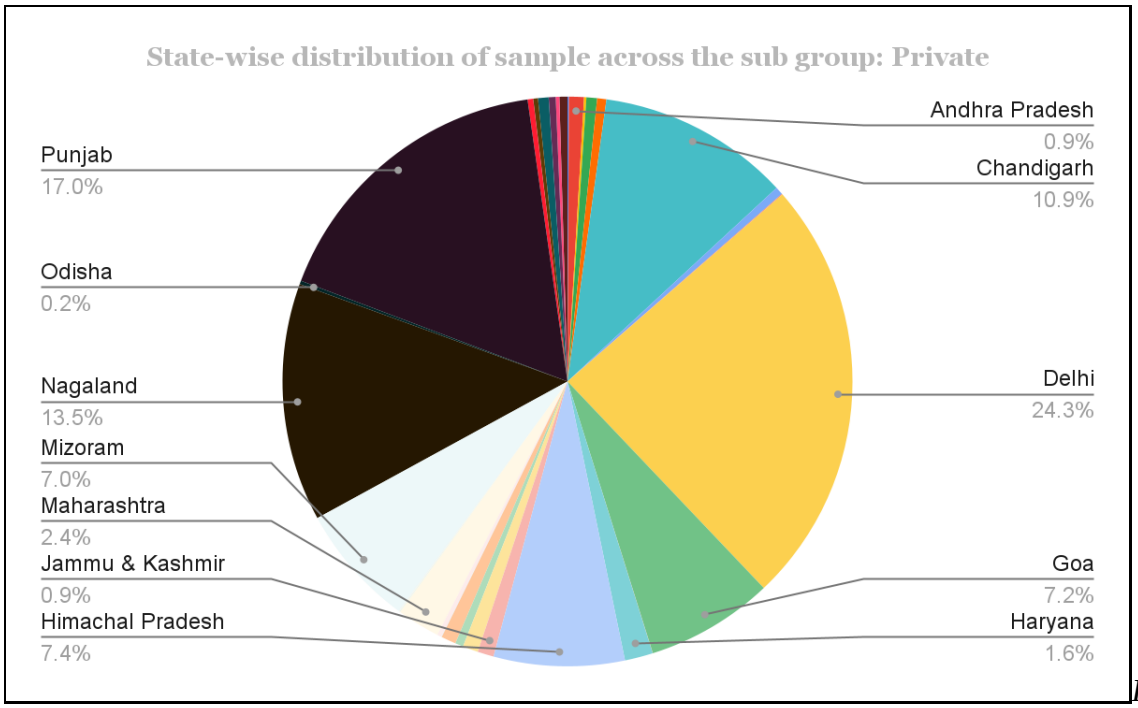


Fig 4.10: State-wise distribution of sample across the sub group: Private

The participation data revealed that from the north eastern states of Nagaland and Mizoram had maximum participation of students belonging to private schools and aided schools respectively. The students of aided schools of Goa has also actively participated in the survey. While looking at the participation of students from different types of schools, Delhi stood first among others.

4.2.1.4: State-wise distribution of sample with regard to Locality of the school

Table 4.4: State-wise distribution of sample with regard to Locality of the school

States	Locality	Response (Number)	Response (Percentage)
Andaman and Nicobar Islands	Rural	93	53.8
	Urban	80	46.2
	Total	173	100.0
Andhra Pradesh	Rural	493	33.7
	Urban	968	66.3
	Total	1461	100.0
Arunachal Pradesh	Rural	65	27.0
	Urban	176	73.0
	Total	241	100.0
Assam	Rural	674	29.8
	Urban	1584	70.2
	Total	2258	100.0
Bihar	Rural	558	38.6
	Urban	887	61.4
	Total	1445	100.0
Chandigarh	Rural	736	18.5
	Urban	3232	81.5
	Total	3968	100.0
Chhattisgarh	Rural	320	22.4
	Urban	1108	77.6
	Total	1428	100.0
Dadra and Nagar Haveli and Daman and Diu	Rural	17	50.0
	Urban	17	50.0
	Total	34	100.0
Delhi	Rural	7618	17.6
	Urban	35590	82.4
	Total	43208	100.0
Goa	Rural	1619	46.9
	Urban	1830	53.1
	Total	3449	100.0
Gujarat	Rural	22	64.7
	Urban	12	35.3
	Total	34	100.0

Haryana	Rural	627	36.5
	Urban	1093	63.5
	Total	1720	100.0
Himachal Pradesh	Rural	2260	64.2
	Urban	1258	35.8
	Total	3518	100.0
Jammu & Kashmir	Rural	779	53.8
	Urban	669	46.2
	Total	1448	100.0
Jharkhand	Rural	1099	41.6
	Urban	1540	58.4
	Total	2639	100.0
Karnataka	Rural	248	20.0
	Urban	990	80.0
	Total	1238	100.0
Kerala	Rural	1260	38.8
	Urban	1987	61.2
	Total	3247	100.0
Ladakh	Rural	5	41.7
	Urban	7	58.3
	Total	12	100.0
Lakshadweep	Rural	5	83.3
	Urban	1	16.7
	Total	6	100.0
Madhya Pradesh	Rural	707	24.8
	Urban	2148	75.2
	Total	2855	100.0
Maharashtra	Rural	657	17.5
	Urban	3092	82.5
	Total	3749	100.0
Manipur	Rural	128	78.0
	Urban	36	22.0
	Total	164	100.0
Meghalaya	Rural	54	56.3
	Urban	42	43.8
	Total	96	100.0
Mizoram	Rural	2491	46.6

	Urban	2859	53.4
	Total	5350	100.0
Nagaland	Rural	626	31.8
	Urban	1341	68.2
	Total	1967	100.0
Odisha	Rural	246	11.6
	Urban	1868	88.4
	Total	2114	100.0
Puducherry	Rural	3	42.9
	Urban	4	57.1
	Total	7	100.0
Punjab	Rural	9197	67.5
	Urban	4428	32.5
	Total	13625	100.0
Rajasthan	Rural	295	28.1
	Urban	755	71.9
	Total	1050	100.0
Sikkim	Rural	7	35.0
	Urban	13	65.0
	Total	20	100.0
Tamil Nadu	Rural	238	29.2
	Urban	577	70.8
	Total	815	100.0
Telangana	Rural	406	22.9
	Urban	1364	77.1
	Total	1770	100.0
Tripura	Rural	14	12.3
	Urban	100	87.7
	Total	114	100.0
Uttar Pradesh	Rural	1184	25.9
	Urban	3396	74.1
	Total	4580	100.0
Uttarakhand	Rural	900	42.2
	Urban	1231	57.8
	Total	2131	100.0
West Bengal	Rural	816	22.1

	Urban	2880	77.9
	Total	3696	100.0

From the above table 4.4, the result shows that Punjab has the highest percentage of samples from rural schools at 67.5%, indicating a strong rural area . On the other hand, Delhi shows a predominantly urban focus with 82.4% of its samples from urban schools.

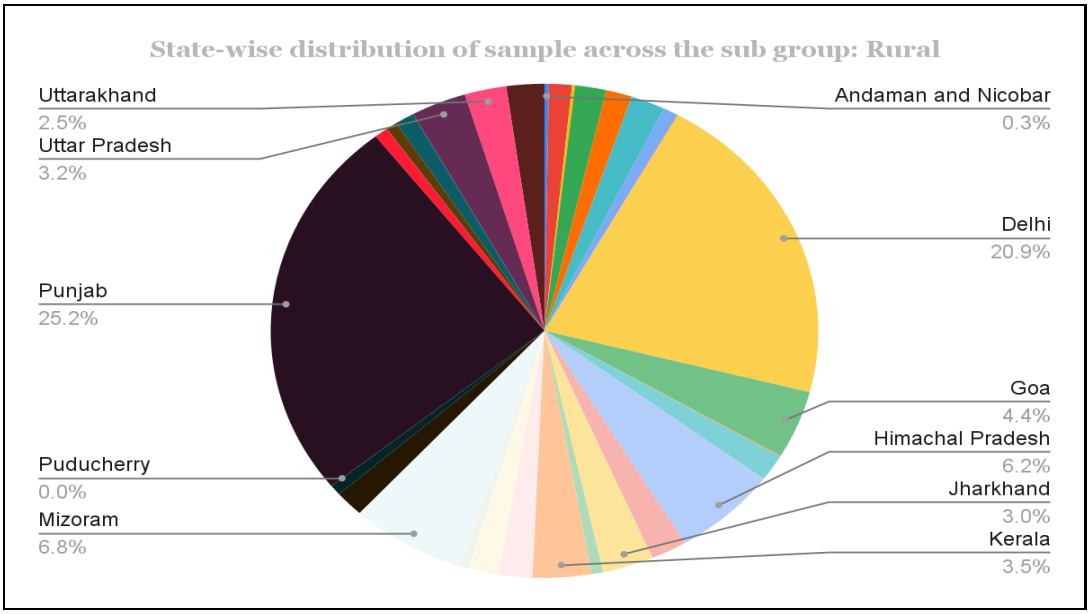


Fig 4.11: State-wise distribution of sample across the sub group: Rural

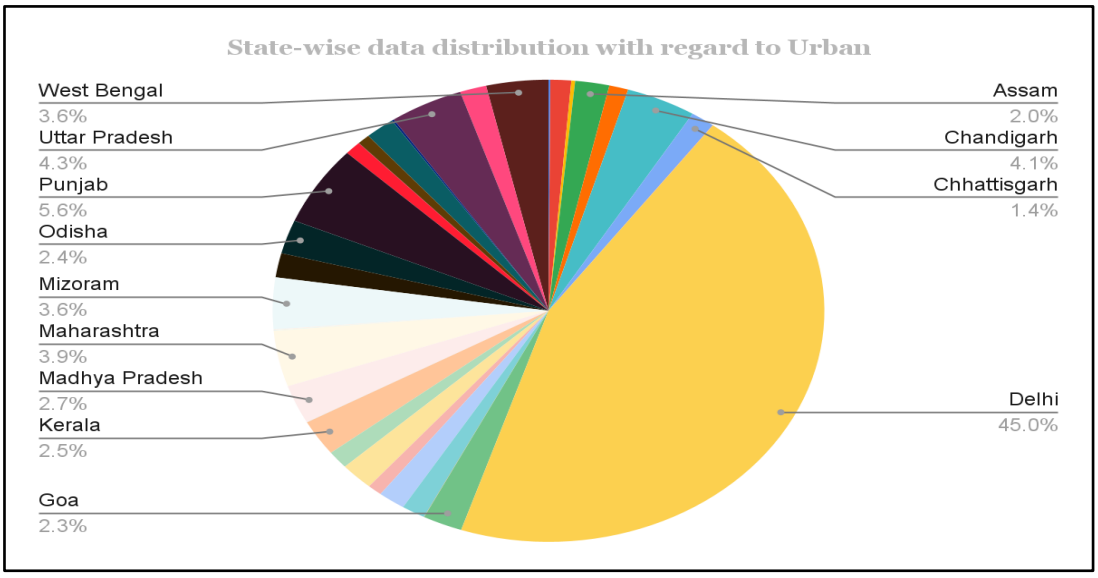


Fig 4.12: State-wise distribution of sample across the sub group: Urban

It is evident from the above section that the majority of students were from Punjab, Delhi irrespective of their locality of the school.

4.2.2 Analysis of Data with Regard to ICT/Digital Exposure

Basic information regarding the availability and use of digital resources and ICT facilities were collected from the sample to understand the nature of exposure of secondary students to ICT and associated aspects. The data collected is analyzed with regard to selected sub groups and is presented systematically in this section.

4.2.2.1: Gender-wise Distribution of Internet access at home

Table 4.5: Gender-wise Distribution of Internet access at home

Gender	Internet access at home		
	Yes	**No**	**Total**
Female	53950 (87.7)	7532 (12.3)	61482 (100.0)
Male	47786 (88.6)	6143 (11.4)	53929 (100.0)
Transgender	177 (80.8)	42 (19.2)	219 (100.0)

From the above table 4.5, the result shows that males have the highest percentage of individuals with internet access at home, at 88.6%. Females closely follow with 87.7%, indicating a slightly lower but still significant adoption rate. In contrast, transgender individuals show a lower percentage at 80.8%.

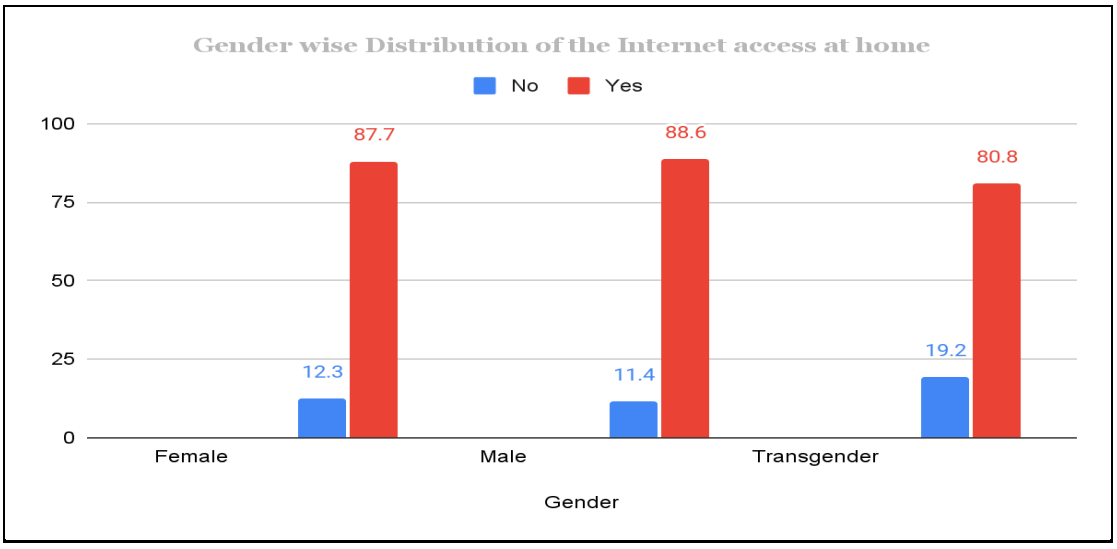


Fig 4.13: Gender-wise Distribution of Internet access at home

4.2.2.2: Gender-wise Distribution of the Email ID

Table 4.6: Gender-wise Distribution of the Email ID

Gender	Distribution of the Email ID		
	Yes	No	Total
Female	42799 (69.6)	18683 (30.4)	61482 (100.0)
Male	43437 (80.5)	10492 (19.5)	53929 (100.0)
Transgender	162 (74.0)	57 (26.0)	219 (100.0)

From the above table 4.6, shows that Males have the highest percentage of individuals with an Email ID (80.5%), followed by transgender individuals (74.0%), and females (69.6%). In terms of not having an Email ID, females have the highest percentage (30.4%), followed by transgender individuals (26.0%), and males (19.5%).

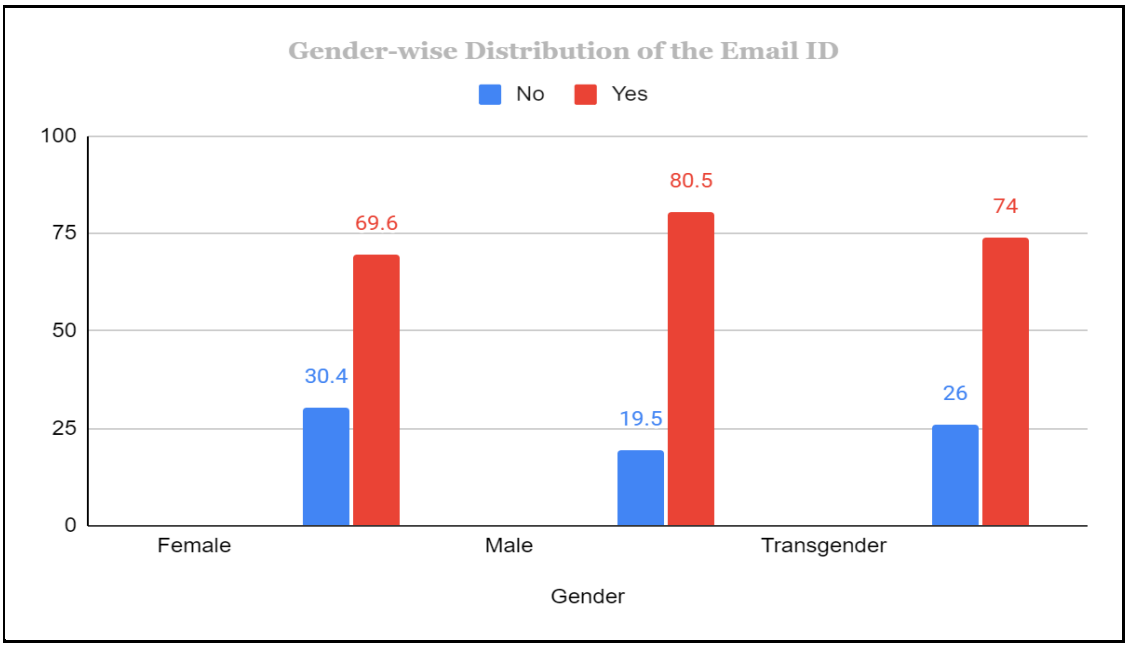


Fig 4.14: Gender-wise data distribution of Email ID

4.2.2.3: Gender-wise Distribution of use of Digital Devices per day

Table 4.7: Gender-wise Distribution of use of Digital Devices per day

Gender	1 hour to 2 hours	2 hours to 4 hours	30 min to 1 hour	Above 4 hours	Do not use it every day	Less than 30 min
Female	15770 (25.6)	7808 (12.7)	17677 (28.8)	3115 (5.1)	5134 (8.4)	11978 (19.5)
Male	14932 (27.7)	7645 (14.2)	15352 (28.5)	3899 (7.2)	3393 (6.3)	8708 (16.1)
Transgender	41 (18.7)	16 (7.3)	42 (19.2)	17 (7.8)	25 (11.4)	78 (35.6)

From the above table 4.7, the result shows that females have the highest percentage (28.8%) use digital devices for 30 minutes to 1 hour daily, indicating a balanced engagement with digital technology for moderate durations. Additionally, 25.6% of females use devices for 1 to 2 hours, suggesting a significant proportion engage in slightly longer sessions. Conversely, males show a similar trend with 28.5% using devices for 30 minutes to 1 hour and 27.7% for 1 to 2 hours, indicating comparable engagement patterns but with a slightly higher percentage in the 1 to 2 hours category compared to females. For transgender individuals, the largest percentage (35.6%) uses digital devices for less than 30 minutes daily, indicating a preference for shorter durations of device use compared to females and males.

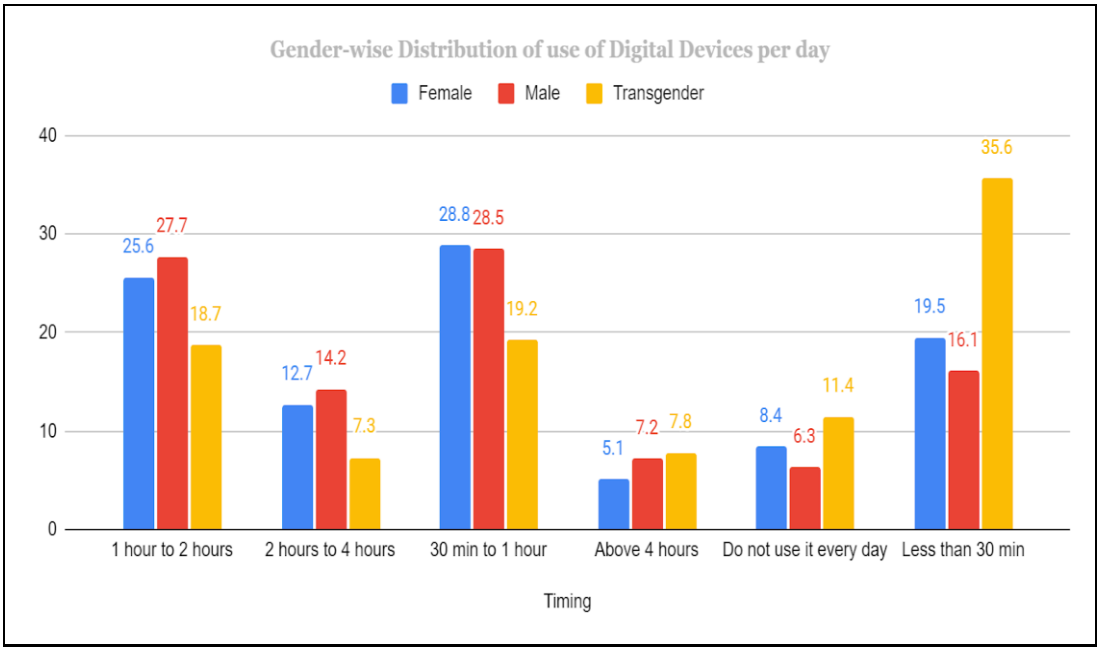


Fig 4.15: Gender-wise data distribution of use of digital devices per day

4.2.2.4: Gender-wise Distribution of Perception about Excessive Screen Time

Table 4.8: Gender-wise Distribution of Perception about Excessive screen time

Gender	1 hour to 2 hours	2 hours to 4 hours	30 min to 1 hour	More than 4 hours	Upto 30 min
Female	11495 (18.7)	8262 (13.4)	14394 (23.4)	7676 (12.5)	19655 (32)
Male	11381 (21.1)	8124 (15.1)	13027 (24.2)	7638 (14.2)	13759 (25.5)
Transgender	34 (15.5)	22 (10)	47 (21.5)	21 (9.6)	95 (43.4)

From the above table 4.8 Females, the largest proportion (32.0%) perceive spending up to 30 minutes on screens, indicating a significant portion adheres to what they consider a moderate screen time limit. Additionally, 18.7% perceive spending 1 to 2 hours on screens, suggesting a balanced perception across different time categories. In contrast, males show a slightly different distribution, with 25.5% perceiving up to 30 minutes and 21.1% perceiving 1 to 2 hours on screens, highlighting a comparable but varied perception compared to females. For transgender individuals, a notable 43.4% perceive spending up to 30 minutes on screens, with smaller percentages perceiving higher screen times.

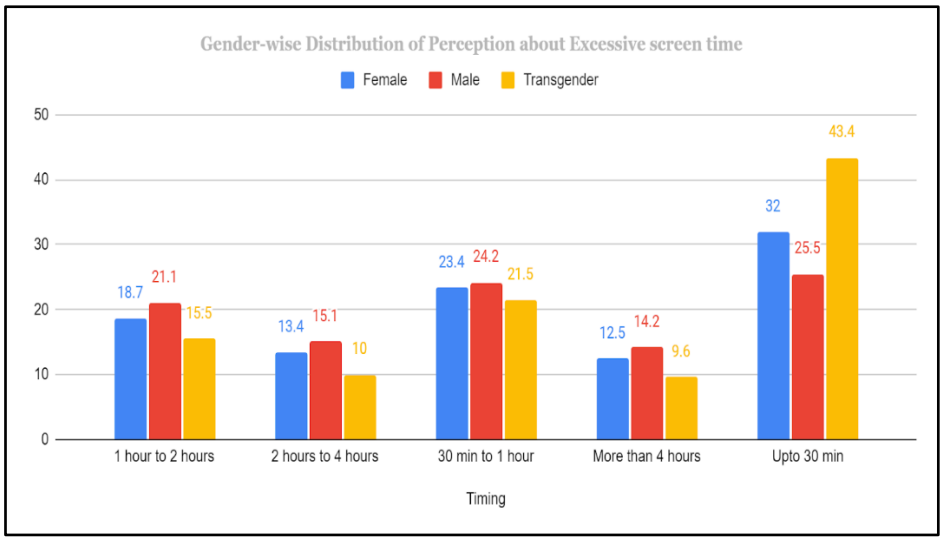


Fig 4.16: Gender-wise data distribution about excessive screen time

4.2.2.5: Gender-wise Distribution of participation in courses related to ICT

Table 4.9: Gender-wise Distribution of participation in courses related to ICT

Gender	Participation in courses related to ICT		
	Yes	**No**	**Total**
Female	29234 (47.5)	32248 (52.5)	61482 (100.0)
Male	25665 (47.6)	28264 (52.4)	53929 (100.0)
Transgender	143 (65.3)	76 (34.7)	219 (100.0)

From the above table 4.9, it is found that transgender individuals emerge with the highest percentage at 65.3%, indicating a significant engagement compared to females at 47.5% and males at 47.6%.

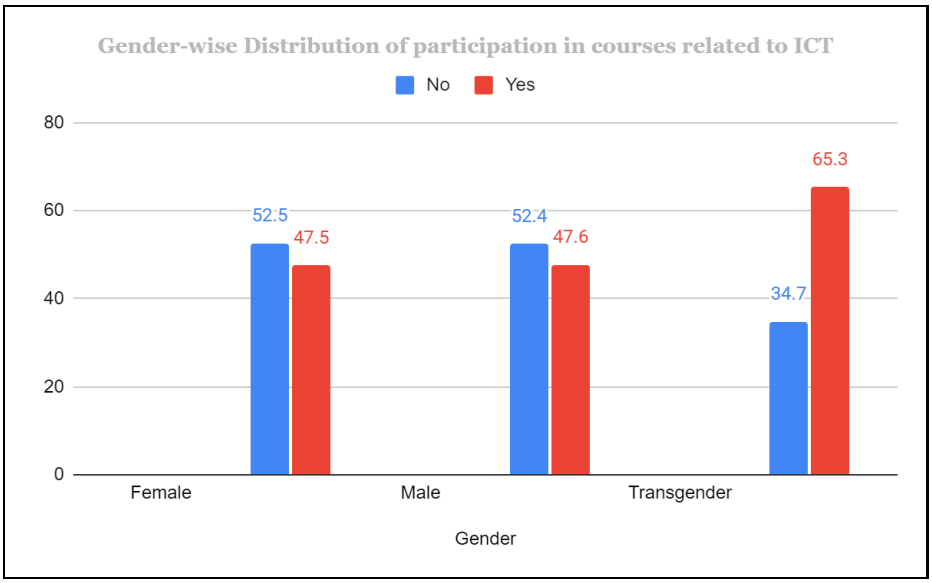


Fig 4.17: Gender-wise Distribution of participation in courses related to ICT

4.2.2.6: Standard wise Distribution of Internet access at home

Table 4.10: Standard-wise Distribution of Internet access at home

Standard	Internet Access at Home		
	Yes	No	Total
10th Standard	33666 (88.4)	4430 (11.6)	38096 (100.0)
11th Standard	4814 (88.3)	636 (11.7)	5450 (100.0)
12th Standard	30022 (88.9)	3754 (11.1)	33776 (100.0)
9th Standard	33412 (87.2)	4896 (12.8)	38308 (100.0)

From the above table 4.10, the 12th standard students have the highest percentage of internet access at 88.9%. Following closely behind are students in the 10th standard, with 88.4% having internet access, showing a similar strong adoption of digital connectivity. In the 11th standard, 88.3% of students have internet access. Among the 9th standard students, 87.2% have internet access, reflecting a slightly lower but still significant level of connectivity compared to higher standards.

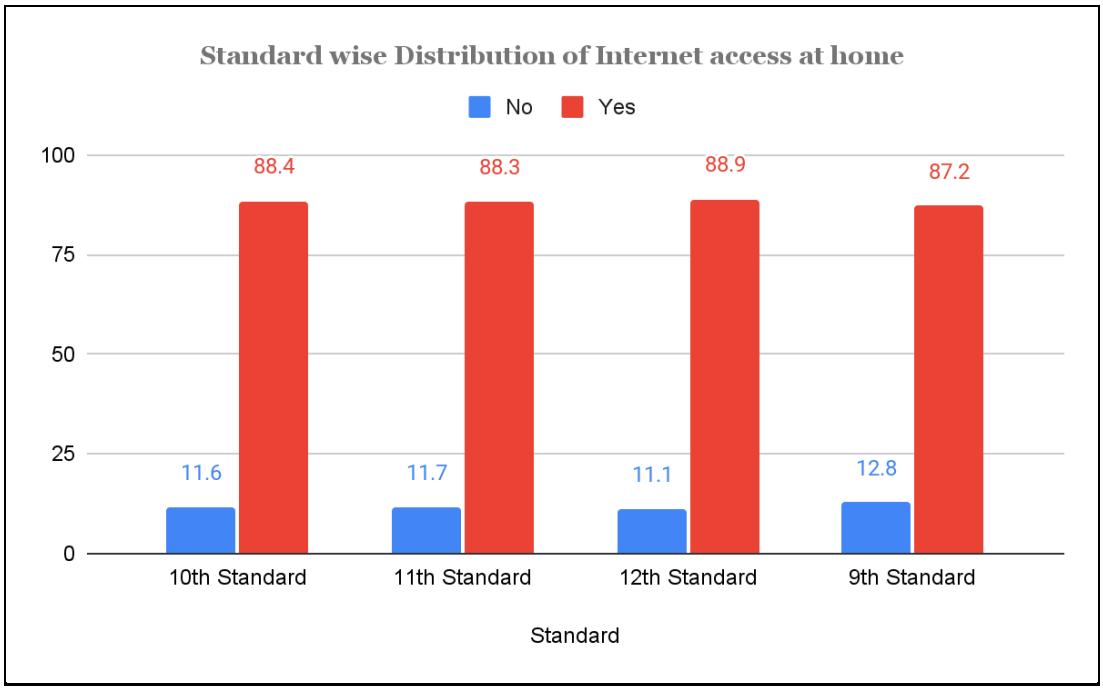


Fig 4.18: Standard-wise Distribution of Internet access at home

4.2.2.7: Standard-wise Distribution of the Email ID

Table 4.11: Standard-wise Distribution of the Email ID

Standard	Distribution of the Email ID		
	Yes	No	Total
10th Standard	28039 (73.6)	10057 (26.4)	38096 (100.0)
11th Standard	4193 (76.9)	1257 (23.1)	5450 (100.0)
12th Standard	27944 (82.7)	5832 (17.3)	33776 (100.0)
9th Standard	26222 (68.5)	12086 (31.5)	38308 (100.0)

From the above table 4.11, Based on the distribution of email IDs among different standards, it is evident that the 12th standard students have the highest percentage of email ID ownership at 82.7%. Following closely behind are students in the 11th standard, with 76.9% having email IDs, showing a substantial engagement with digital platforms for communication. In the 10th standard, 73.6% of students possess email IDs, reflecting a significant presence but slightly lower than the upper secondary levels. Among the 9th standard students, 68.5% have email IDs, demonstrating a growing but relatively lower uptake compared to higher standards.

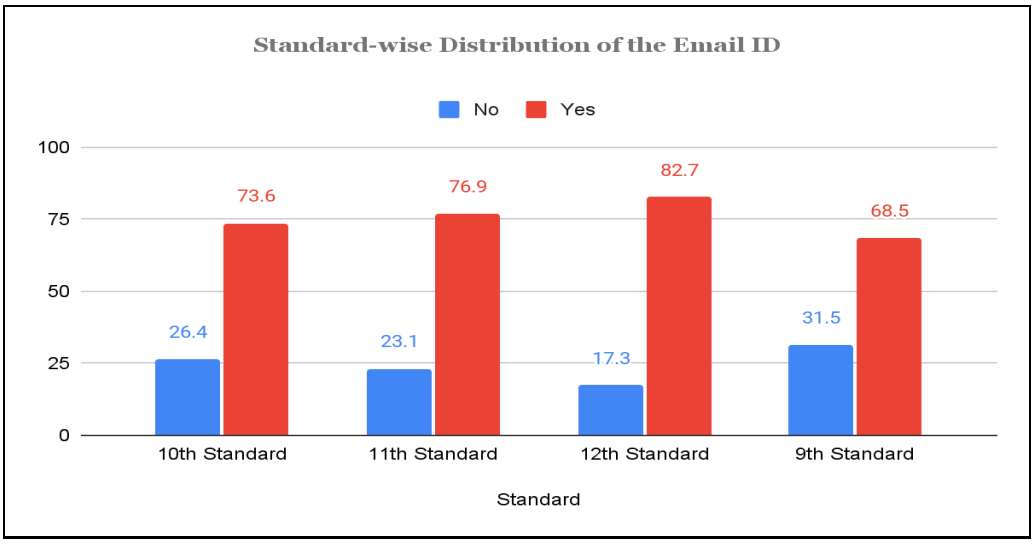


Fig 4.19: Standard-wise Distribution of the Email ID

4.2.2.8: Standard-wise Distribution of Use of Digital Devices per day

Table 4.12: Standard-wise Distribution of Use of Digital Devices per day

Standard	1 hour to 2 hours	2 hours to 4 hours	30 min to 1 hour	Above 4 hours	Do not use it every day	Less than 30 min
9th standard	9423 (24.6)	3841 (10)	11874 (31)	1519 (4)	3241 (8.5)	8410 (22)
10th standard	10150 (26.6)	4682 (12.3)	11350 (29.8)	1880 (4.9)	3010 (7.9)	7024 (18.4)
11th standard	1339 (24.6)	760 (13.9)	1554 (28.5)	383 (7)	382 (7)	1031 (18.9)
12th standard	9831 (29.1)	6185 (18.3)	8293 (24.6)	3249 (9.6)	1919 (5.7)	4299 (12.7)

From the above table 4.12, 10th Standard has the highest percentage of students spending 1 hour to 2 hours on digital devices per day is 26.6%. 11th Standard has 24.6% of students spending 1 hour to 2 hours on digital devices daily, which is the highest among the given categories. 12th Standard has the highest percentage here also for 1 hour to 2 hours, at 29.1%. 9th Standard has the highest percentage for 1 hour to 2 hours, with 24.6%.

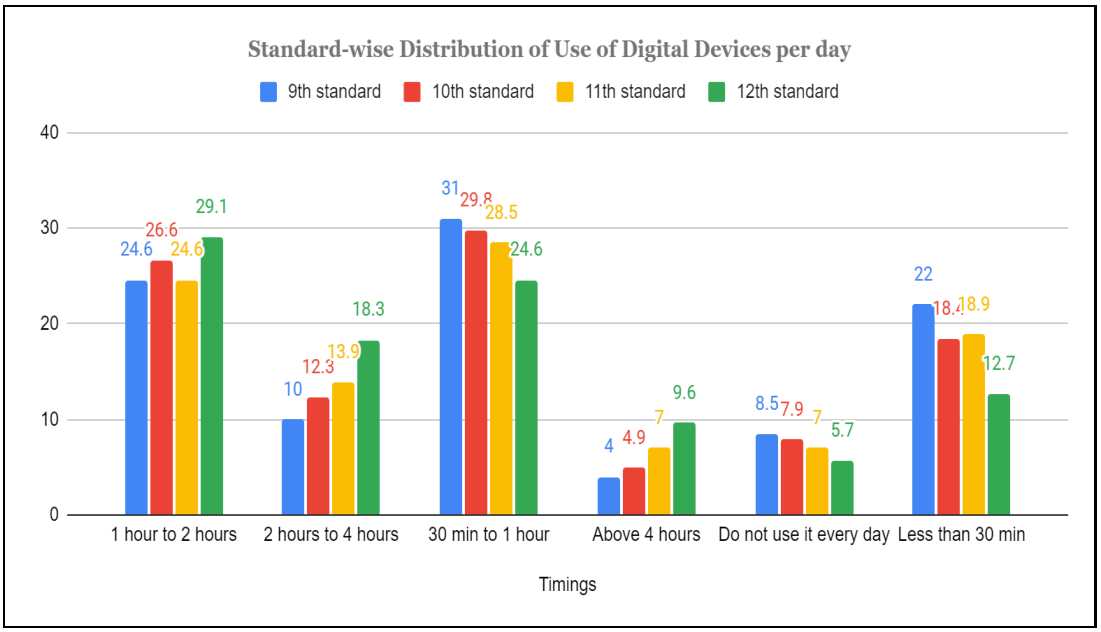


Fig 4.20: Standard-wise Distribution of Use of Digital Devices per day

4.2.2.9: Standard-wise Distribution of Excessive screen time

Table 4.13: Standard-wise Distribution of Excessive screen time

Timings	1 hour to 2 hours	2 hours to 4 hours	30 min to 1 hour	More than 4 hours	Upto 30 min
10th standard	7645 (20.1)	5388 (14.1)	9355 (24.6)	4432 (11.6)	11276 (29.6)
11th standard	1035 (19)	729 (13.4)	1238 (22.7)	830 (15.2)	1618 (29.7)
12th standard	6834 (20.2)	5698 (16.9)	7096 (21)	6483 (19.2)	7665 (22.7)
9th standard	7396 (19.3)	4593 (12)	9779 (25.5)	3590 (9.4)	12950 (33.8)

From the above table 4.13, the result indicates that 10th standard has the highest percentage of students spending 1 hour to 2 hours on screen time, with 20.1% falling within this range. 2 hours to 4 hours is most prevalent among students in the 12th standard, with 16.9% of them spending this amount of time on screens. 30 minutes to 1 hour of screen time is notably observed across different standards, with significant percentages. For instance, in the 10th standard, 24.6% of students fall within this range, while in the 11th standard, 22.7% do. In the 9th standard, it accounts for 25.5% of students, and in the 12th Grade, it constitutes 21.0% of students. More than 4 hours is the highest category for screen time in the 12th standard, with 19.2% of students falling into this range. Among the standards surveyed, the 9th standard shows the highest percentage of students spending 30 minutes to 1 hour on screen time, with 25.5% falling within this range.

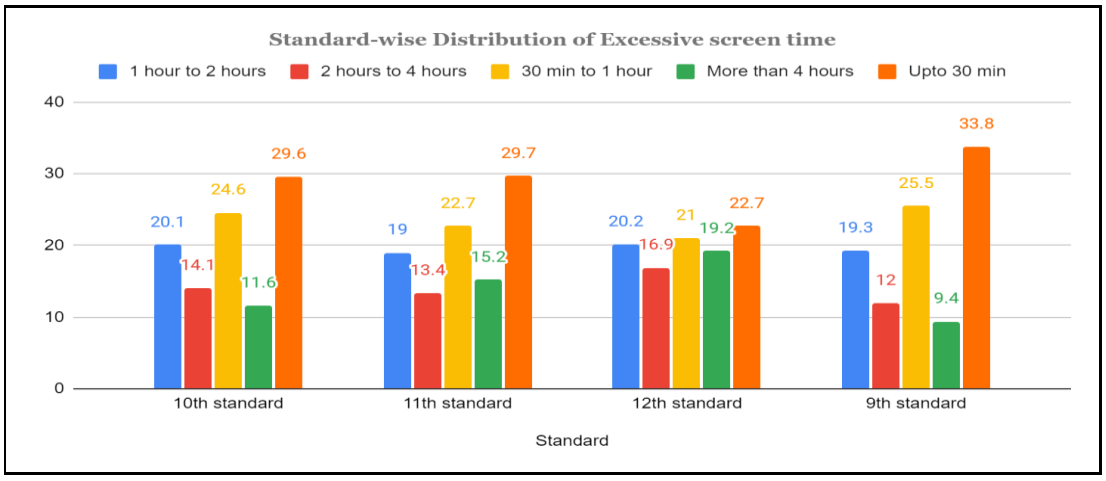


Fig 4.21: Standard-wise Distribution of Excessive screen time

4.2.2.10: Standard-wise Distribution of participation in courses related to ICT

Table 4.14: Standard-wise Distribution of participation in courses related to ICT

Standard	Participation in courses related to ICT		
	Yes	No	Total
10th Standard	19341 (50.8)	18755 (49.2)	38096 (100.0)
11th Standard	2906 (53.3)	2544 (46.7)	5450 (100.0)
12th Standard	15938 (47.2)	17838 (52.8)	33776 (100.0)
9th Standard	16857 (44.0)	21451 (56.0)	38308 (100.0)

From the above table 4.14, the result indicates that, In the 10th standard, 50.8% of students participate in courses related to ICT, compared to 53.3% in the 11th standard, 47.2% in the 12th standard, and 44.0% in the 9th standard. This reveals varying levels of engagement across different grade levels, with higher participation rates observed in the 11th standard compared to the 12th and 9th standards. These percentages highlight the distribution of ICT course participation among students at different stages of their secondary education, underscoring potential differences in curriculum integration and student interest across these standards.

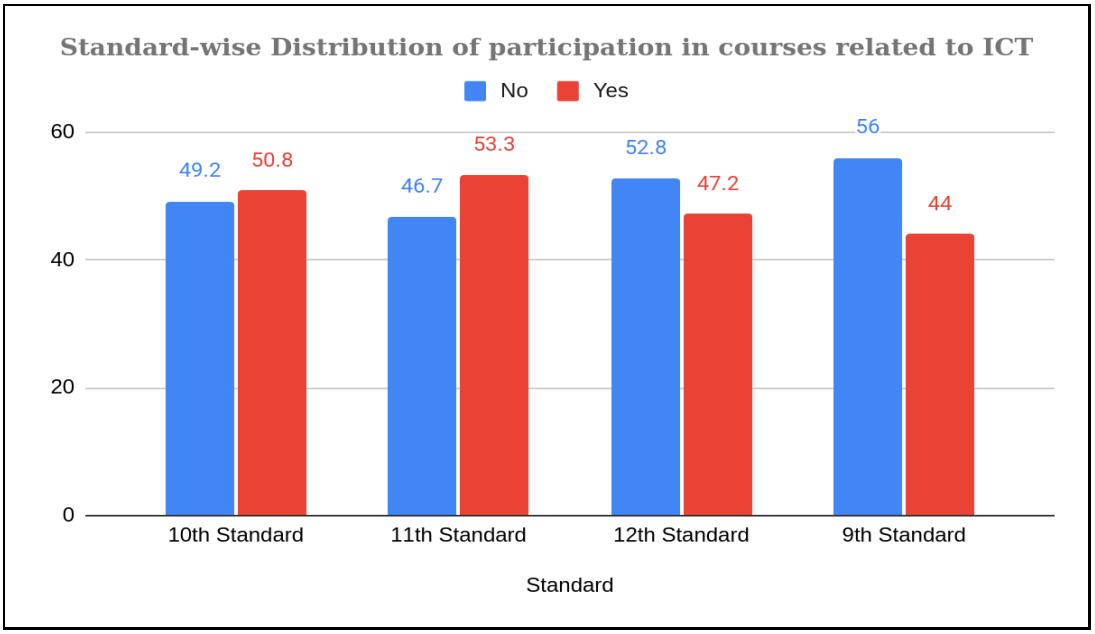


Fig 4.22: Standard-wise Distribution of participation in courses related to ICT

4.2.2.11: Type of School-wise Distribution of Internet Access at Home

Table 4.15: Type of School wise Distribution of Internet Access at Home

Type of School	Internet Access at Home		
	Yes	No	Total
Aided School	5770 (88.5)	748 (11.5)	6518 (100.0)
Government	85038 (87.6)	11990 (12.4)	97028 (100.0)
Private	11105 (91.9)	979 (8.1)	12084 (100.0)

From the above table 4.15, In aided schools, 88.5% of students have internet access at home, while in government schools, this figure is higher at 87.6%, and in private schools, it is highest at 91.9%. This indicates that a significant majority of students across all types of schools have access to the internet from their homes, facilitating online learning, research, and connectivity. The data underscores the importance of digital access in education, ensuring students can effectively engage with online resources and educational materials outside of school hours.

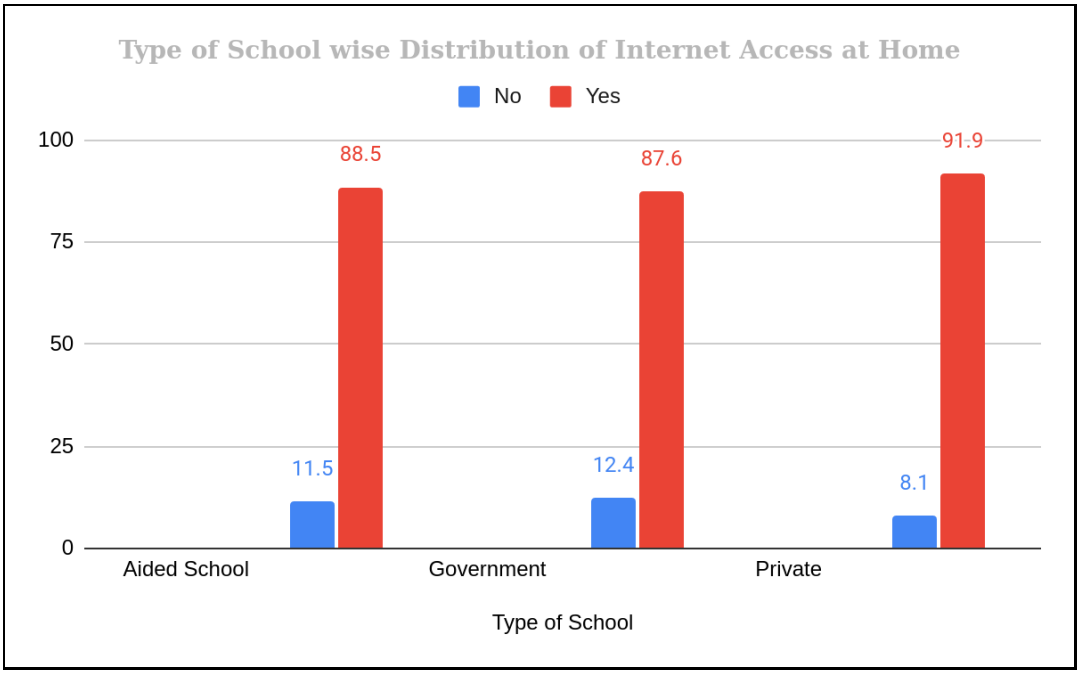


Fig 4.23: Type of School wise Distribution of Internet Access at Home

4.2.2.12: Type of School-wise Distribution of the Email ID

Table 4.16: Type of School-wise Distribution of the Email ID

Type of School	Distribution of the Email ID		
	Yes	No	Total
Aided School	5015 (76.9)	1503 (23.1)	6518 (100.0)
Government	72707 (74.9)	24321 (25.1)	97028 (100.0)
Private	8676 (71.8)	3408 (28.2)	12084 (100.0)

From the above table 4.16, In aided schools, 76.9% of students have personal email IDs, while in government schools, 74.9% have them, and in private schools, 71.8% do. This indicates a generally high adoption of email IDs across all types of schools, with aided schools showing the highest percentage. The data suggests that email usage for communication and educational purposes is prevalent among students across different school types, contributing to their digital connectivity and communication skills development.

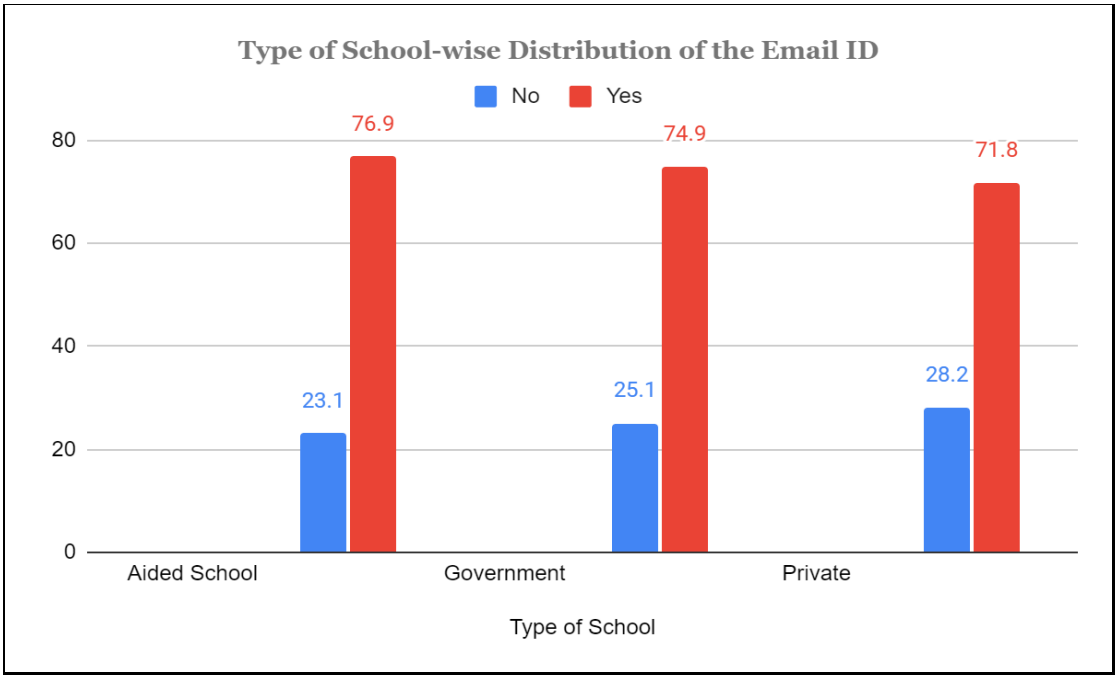


Fig 4.24: Type of School-wise Distribution of the Email ID

4.2.2.13: Type of School-wise Distribution of Digital Devices Used per Day

Table 4.17: Type of School-wise Distribution of Digital Devices Used per Day

Type of School	1 hour to 2 hours	2 hours to 4 hours	30 min to 1 hour	Above 4 hours	Do not use it every day	Less than 30 min
Aided School	1781 (27.3)	1083 (16.6)	1856 (28.5)	433 (6.6)	469 (7.2)	896 (13.7)
Government	25550 (26.3)	12526 (12.9)	12526 (28.7)	5856 (6)	7155 (7.4)	18071 (18.6)
Private	3412 (28.2)	1860 (15.4)	3345 (27.7)	742 (6.1)	928 (7.7)	1797 (14.9)

From the above table 4.17, In aided schools, a significant portion of students allocate their daily digital device usage as follows: 27.3% spend 1 to 2 hours, 16.6% use devices for 2 to 4 hours, and 28.5% engage for 30 minutes to 1 hour. Government schools show a similar pattern with 26.3% using devices for 1 to 2 hours, 28.7% for 30 minutes to 1 hour, and 18.6% for less than 30 minutes daily. Meanwhile, in private schools, 28.2% of students use devices for 1 to 2 hours daily, 27.7% for 30 minutes to 1 hour, and 15.4% for 2 to 4 hours.

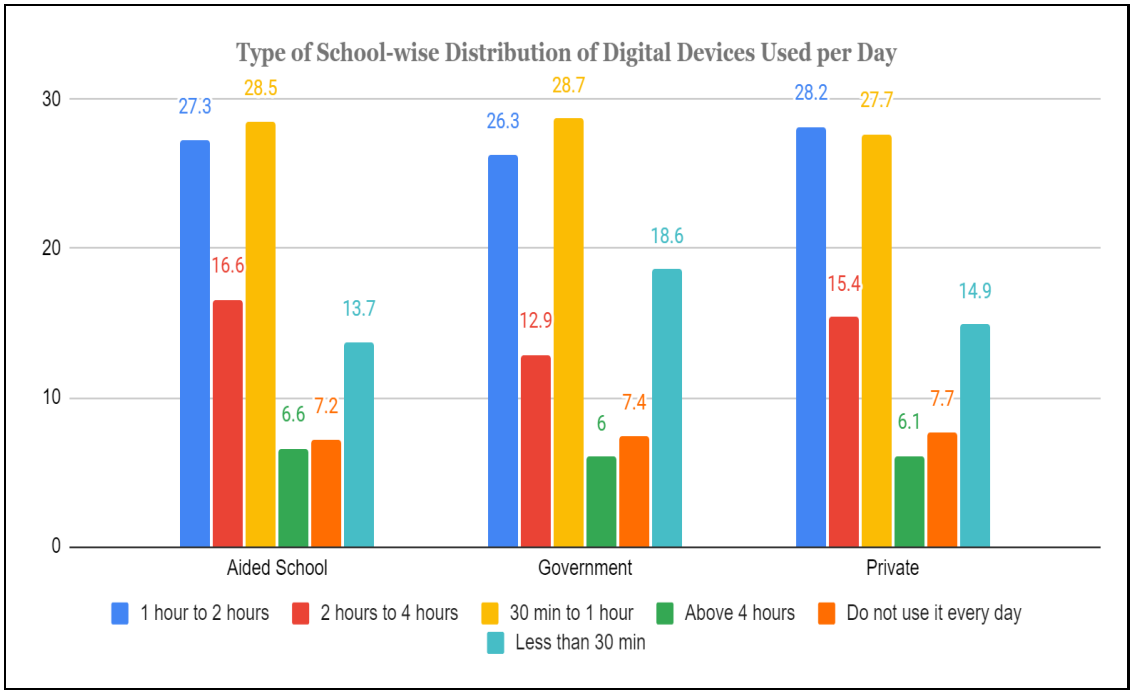


Fig 4.25: Type of School wise Distribution of Digital Devices Used per Day

4.2.2.14: Type of School wise Distribution of Excessive Screen Time

Table 4.18: Type of School wise Distribution of Excessive Screen Time

Timing	1 hour to 2 hours	2 hours to 4 hours	30 min to 1 hour	More than 4 hours	Upto 30 min
Aided School	1277 (19.6)	980 (15)	1484 (22.8)	1212 (18.6)	1565 (24)
Government	19275 (19.9)	13270 (13.7)	23391 (24.1)	12075 (12.4)	29017 (29.9)
Private	2358 (19.5)	2158 (17.9)	2593 (21.5)	2048 (16.9)	2927 (24.2)

From the above table 4.18, In aided schools, the distribution of excessive screen time shows that 24.0% of students spend up to 30 minutes, 22.8% spend 30 minutes to 1 hour, and 19.6% spend 1 to 2 hours on screens. Government schools report that 29.9% of students spend up to 30 minutes, 24.1% spend 30 minutes to 1 hour, and 19.9% spend 1 to 2 hours on screens. Private schools indicate that 24.2% of students spend up to 30 minutes, 21.5% spend 30 minutes to 1 hour, and 19.5% spend 1 to 2 hours on screens.

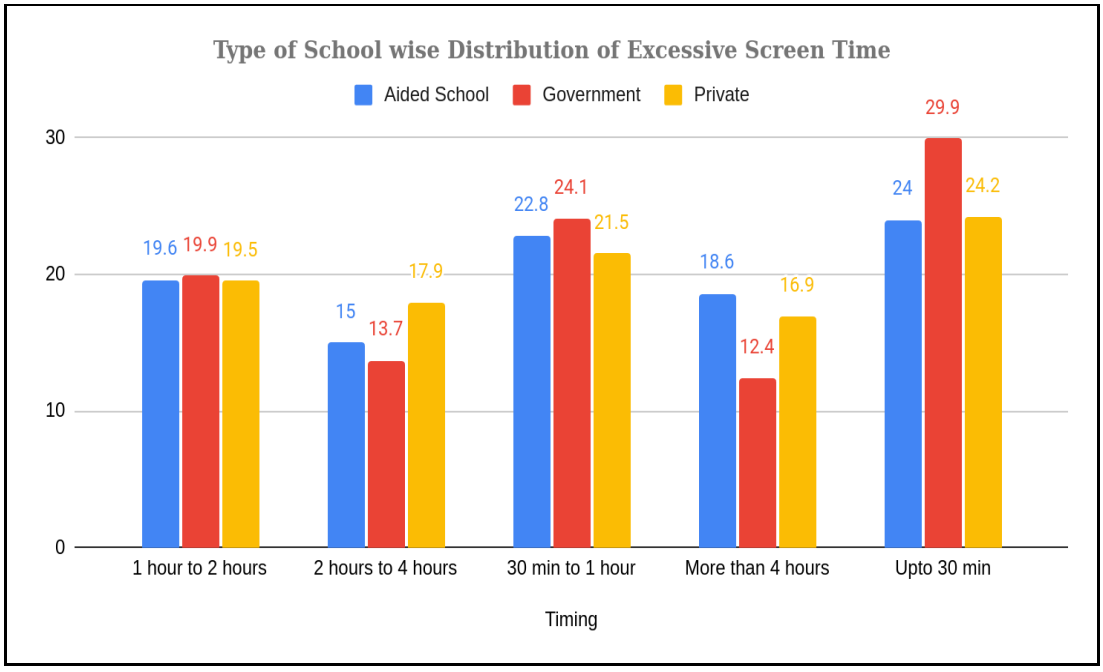


Fig 4.26: Type of School wise Distribution of Excessive Screen Time

4.2.2.15: Type of School wise Distribution of courses related to ICT

Table 4.19: Type of School-wise Distribution of Courses Related to ICT

Type of School	Distribution of courses related to ICT		
	Yes	No	Total
Aided School	2666 **(**40.9**)**	3852 (59.1)	6518 (100.0)
Government	46707 **(**48.1**)**	50321 **(**51.9**)**	97028 (100.0)
Private	5669 **(**46.9**)**	6415 **(**53.1**)**	12084 (100.0)

From the above table 4.19, In aided schools, 40.9% offer courses related to ICT, while 59.1% do not, Government schools show a nearly equal distribution, with 48.1% offering ICT courses and 51.9% not offering them, Among private schools, 46.9% provide ICT courses, while 53.1% do not.

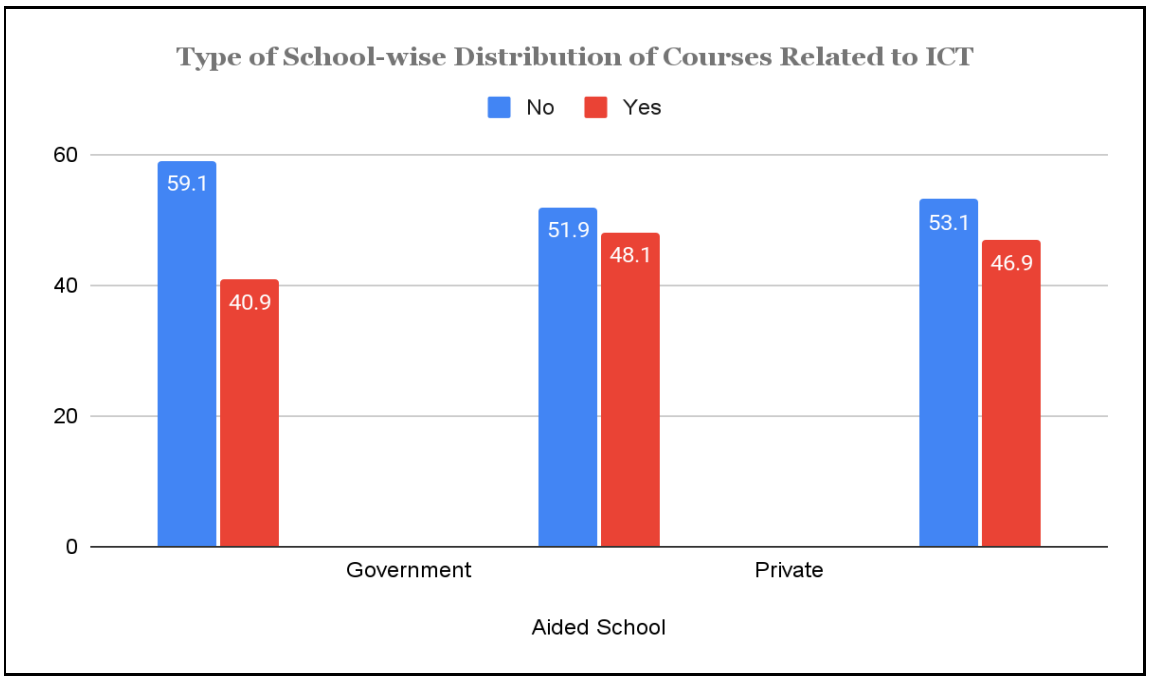


Fig 4.27: Type of School wise Distribution of courses related to ICT

4.2.2.16: Locality-wise Distribution of Internet access at home

Table 4.20: Locality-wise Distribution of Internet access at home

Locality	Internet Access at Home		
	Yes	No	Total
Rural	31605 (86.7)	4862 (13.3)	36467 (100.0)
Urban	70308 (88.8)	8855 (11.2)	79163 (100.0)

From Table 4.20, In Rural Areas, 86.7% of respondents have internet access at home, 13.3% do not have internet access at home. And in Urban Areas, 88.8% of respondents have internet access at home, 11.2% do not have internet access at home. This indicates that a higher percentage of people in both rural and urban areas have internet access at home, with urban areas showing a slightly higher access rate compared to rural areas.

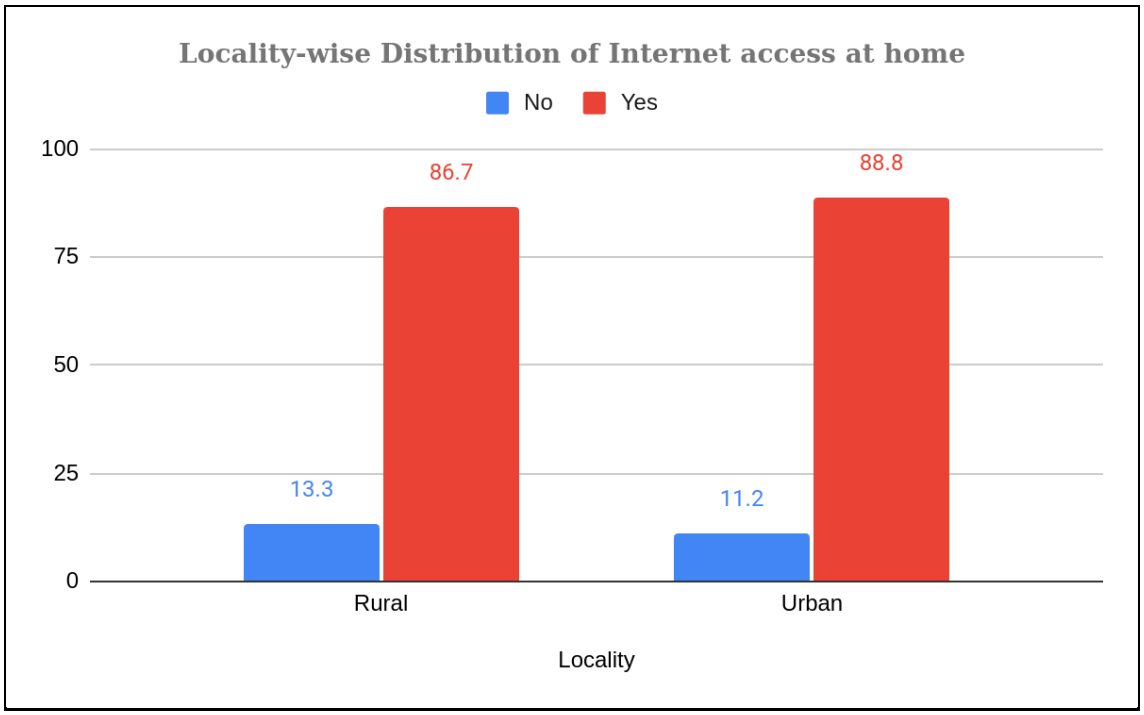


Fig 4.28: Locality-wise Distribution of Internet access at home

4.2.2.17: Locality-wise Distribution of Email ID

Table 4.21: Locality-wise Distribution of Email ID

Locality	Distribution of the Email ID		
	Yes	**No**	**Total**
Rural	26598 **(**72.9**)**	9869 **(**27.1**)**	36467 (100.0)
Urban	59800 **(**75.5**)**	19363 **(**24.5**)**	79163 (100.0)

From Table 4.21 in Rural Areas, 72.9% of respondents have a personal email ID, 27.1% do not have a personal email ID. and Urban Areas, 75.5% of respondents have a personal email ID, 24.5% do not have a personal email ID. This shows that a higher percentage of people in urban areas have personal email IDs compared to rural areas, where a significant but slightly lower percentage also have access to personal email services.

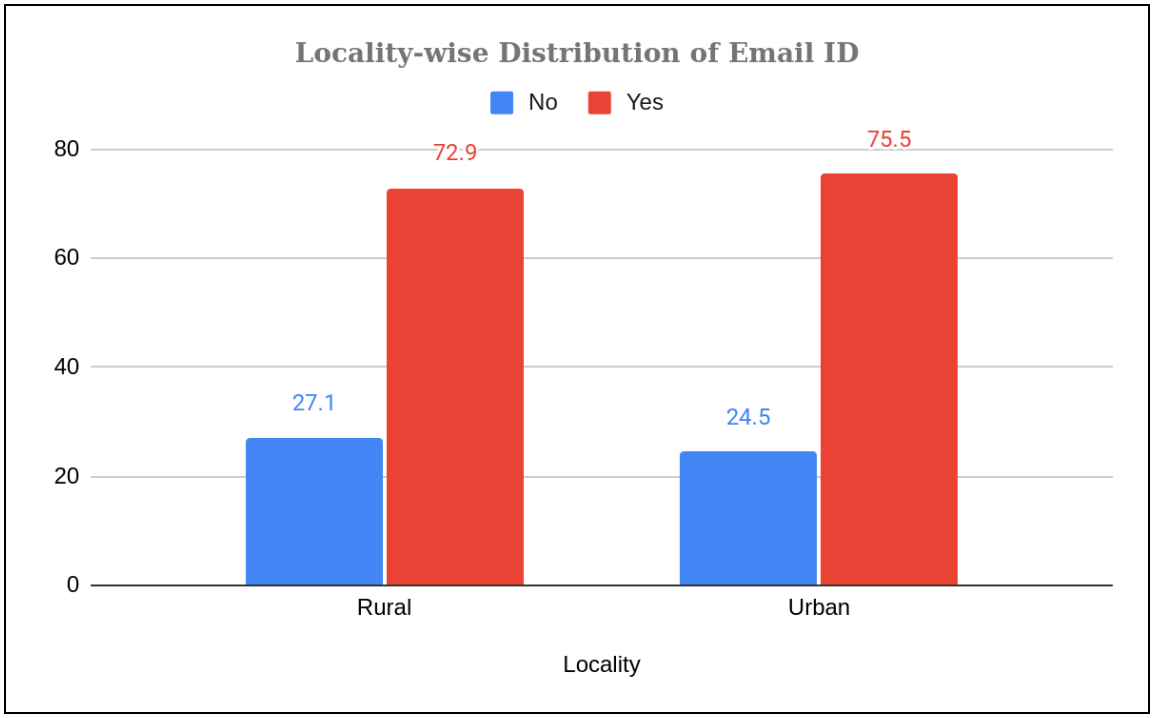


Fig 4.29: Locality-wise Distribution of Email ID

4.2.2.18: Locality-wise Distribution of Digital Devices Used per day

Table 4.22: Locality-wise Distribution of Digital Devices Used per day

Timing	1 hour to 2 hours	2 hours to 4 hours	30 min to 1 hour	Above 4 hours	Do not use it every day	Less than 30 min
Rural	8758 (24)	3841 (10.5)	10755 (29.5)	1947 (5.3)	3008 (8.2)	8158 (22.4)
Urban	21985 (27.8)	11628 (14.7)	22316 (28.2)	5084 (6.4)	5544 (7)	12606 (15.9)

From Table 4.22, the result indicates that

Rural Areas:

- 24.0% of respondents use digital devices for 1 to 2 hours per day.
- 29.5% use devices for 30 minutes to 1 hour per day.
- 22.4% use devices for less than 30 minutes per day.
- Other usage categories include 10.5% for 2 to 4 hours, 8.2% do not use devices every day, and 5.3% use devices for more than 4 hours daily.

Urban Areas:

- 27.8% of respondents use digital devices for 1 to 2 hours per day.
- 28.2% use devices for 30 minutes to 1 hour per day.
- 15.9% use devices for less than 30 minutes per day.
- Other usage categories include 14.7% for 2 to 4 hours, 7.0% do not use devices every day, and 6.4% use devices for more than 4 hours daily.

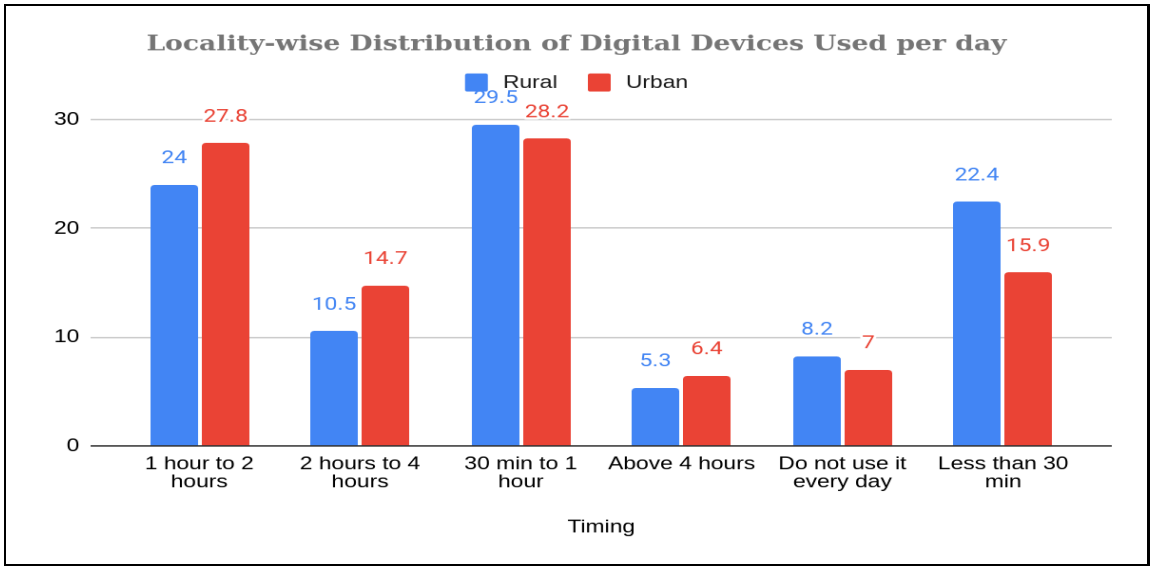


Fig 4.30: Locality-wise Distribution of Digital Devices Used per day

4.2.2.19: Locality-wise Distribution of Excessive Screen Time

Table 4.23: Locality-wise Distribution of Excessive screen time

Timing	1 hour to 2 hours	2 hours to 4 hours	30 min to 1 hour	More than 4 hours	Upto 30 min
Rural	6800 (18.6)	3759 (10.3)	9506 (26.1)	3341 (9.2)	13061 (35.8)
Urban	16110 (20.4)	12649 (16)	17962 (22.7)	11994 (15.2)	20448 (25.8)

From table 4.23 the result indicates, In rural areas, the majority of respondents spend up to 30 minutes (35.8%) and between 30 minutes to 1 hour (26.1%) on excessive screen time, followed by 1 to 2 hours (18.6%). Fewer respondents spend more than 4 hours (9.2%) or between 2 to 4 hours (10.3%) on excessive screen time. In urban areas, a similar trend is observed with the majority spending up to 30 minutes (25.8%) and between 30 minutes to 1 hour (22.7%) on excessive screen time. A significant portion also spends 1 to 2 hours (20.4%), while fewer spend more than 4 hours (15.2%) or between 2 to 4 hours (16.0%).

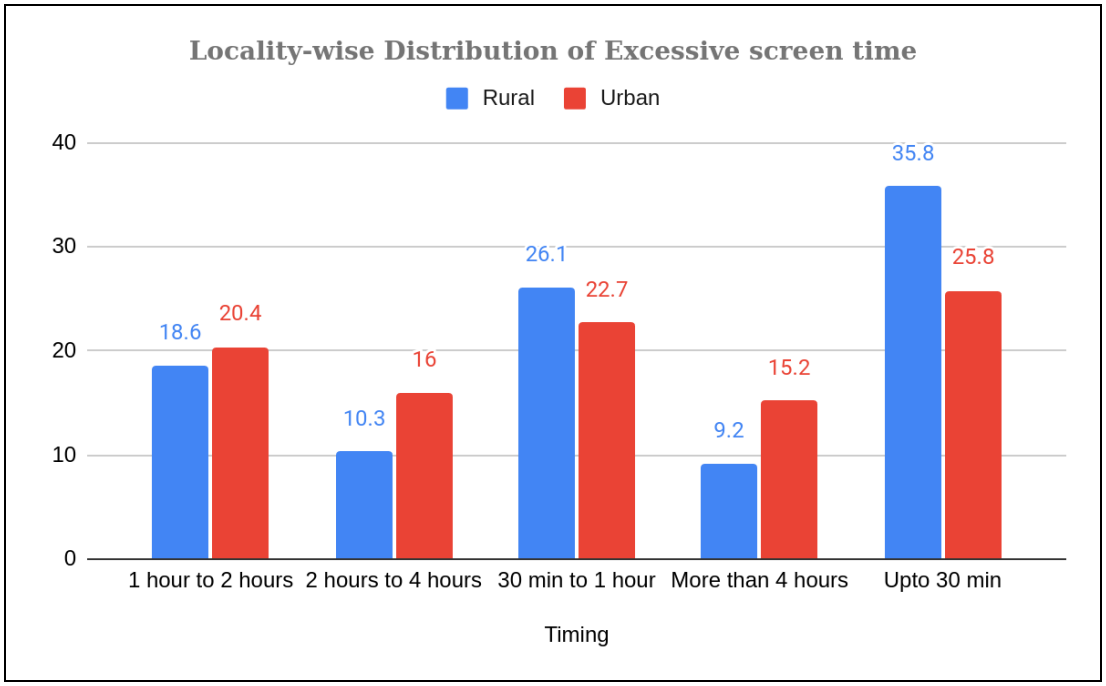


Fig 4.31: Locality-wise Distribution of Excessive screen time

4.2.2.20: Locality-wise Distribution of courses related to ICT

Table 4.24: Locality-wise Distribution of courses related to ICT

Locality	Distribution of Courses related to ICT		
	Yes	No	Total
Rural	19216 (52.7)	17251 (47.3)	36467 (100.0)
Urban	35826 (45.3)	43337 (54.7)	79163 (100.0)

From the above table 4.24, the result indicates that,

- In rural areas, 52.7% of respondents indicated access to courses related to ICT, while 47.3% did not.
- In urban areas, a lower percentage (45.3%) reported access to ICT courses compared to rural areas, where 54.7% did not.

This suggests that while there is a significant uptake of ICT courses in both rural and urban areas, rural areas show slightly higher engagement in ICT education compared to urban areas

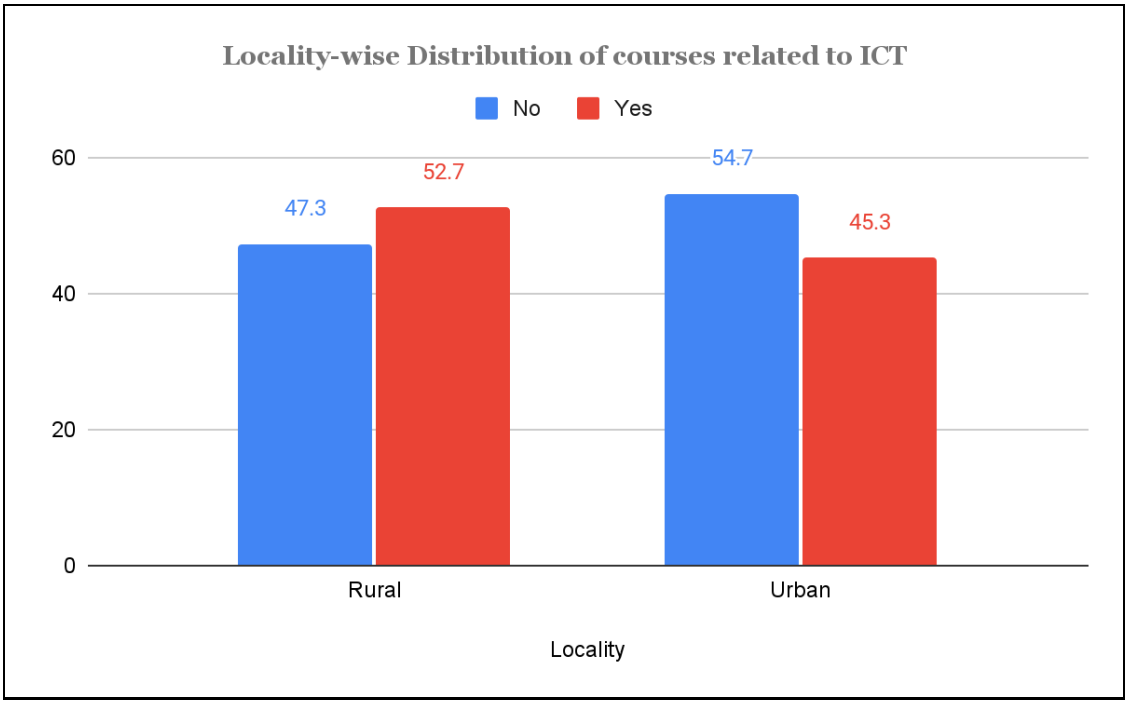


Fig 4.32: Locality-wise Distribution of courses related to ICT

4.2.2.21: State-wise Distribution of Internet access at home

Table 4.25: State-wise Distribution of Internet access at home

States	Internet access at home	Response (Number)	Response (Percentage)
Andaman and Nicobar Islands	No	16	9.2
	Yes	157	90.8
	Total	173	100.0
Andhra Pradesh	No	274	18.8
	Yes	1187	81.2
	Total	1461	100.0
Arunachal Pradesh	No	21	8.7
	Yes	220	91.3
	Total	241	100.0
Assam	No	183	8.1
	Yes	2075	91.9
	Total	2258	100.0
Bihar	No	189	13.1
	Yes	1256	86.9
	Total	1445	100.0
Chandigarh	No	403	10.2
	Yes	3565	89.8

	Total	3968	100.0
Chhattisgarh	No	129	9.0
	Yes	1299	91.0
	Total	1428	100.0
Dadra and Nagar Haveli and Daman and Diu	No	10	29.4
	Yes	24	70.6
	Total	34	100.0
Delhi	No	6064	14.0
	Yes	37144	86.0
	Total	43208	100.0
Goa	No	391	11.3
	Yes	3058	88.7
	Total	3449	100.0
Gujarat	No	7	20.6
	Yes	27	79.4
	Total	34	100.0
Haryana	No	242	14.1
	Yes	1478	85.9
	Total	1720	100.0
Himachal Pradesh	No	391	11.1
	Yes	3127	88.9
	Total	3518	100.0
Jammu & Kashmir	No	223	15.4
	Yes	1225	84.6
	Total	1448	100.0
Jharkhand	No	278	10.5
	Yes	2361	89.5
	Total	2639	100.0
Karnataka	No	148	12.0
	Yes	1090	88.0
	Total	1238	100.0
Kerala	No	301	9.3
	Yes	2946	90.7
	Total	3247	100.0
Ladakh	No	3	25.0
	Yes	9	75.0
	Total	12	100.0

Lakshadweep	No	6	100.0
Madhya Pradesh	No	322	11.3
	Yes	2533	88.7
	Total	2855	100.0
Maharashtra	No	337	9.0
	Yes	3412	91.0
	Total	3749	100.0
Manipur	No	17	10.4
	Yes	147	89.6
	Total	164	100.0
Meghalaya	No	14	14.6
	Yes	82	85.4
	Total	96	100.0
Mizoram	No	274	5.1
	Yes	5076	94.9
	Total	5350	100.0
Nagaland	No	187	9.5
	Yes	1780	90.5
	Total	1967	100.0
Odisha	No	147	7.0
	Yes	1967	93.0
	Total	2114	100.0
Puducherry	No	2	28.6
	Yes	5	71.4
	Total	7	100.0
Punjab	No	1694	12.4
	Yes	11931	87.6
	Total	13625	100.0
Rajasthan	No	103	9.8
	Yes	947	90.2
	Total	1050	100.0
Sikkim	No	1	5.0
	Yes	19	95.0
	Total	20	100.0
Tamil Nadu	No	115	14.1
	Yes	700	85.9
	Total	815	100.0

Telangana	No	225	12.7
	Yes	1545	87.3
	Total	1770	100.0
Tripura	No	8	7.0
	Yes	106	93.0
	Total	114	100.0
Uttar Pradesh	No	472	10.3
	Yes	4108	89.7
	Total	4580	100.0
Uttarakhand	No	229	10.7
	Yes	1902	89.3
	Total	2131	100.0
West Bengal	No	297	8.0
	Yes	3399	92.0
	Total	3696	100.0

From the above table 4.25, Mizoram has the highest percentage of households with internet access at home at 94.9%. States like Delhi (86.0%) and Kerala (90.7%) also show a high prevalence of internet access.

Conversely, states such as Andaman and Nicobar Islands (90.8%) and Arunachal Pradesh (91.3%) also have significant percentages but lower than the national average.

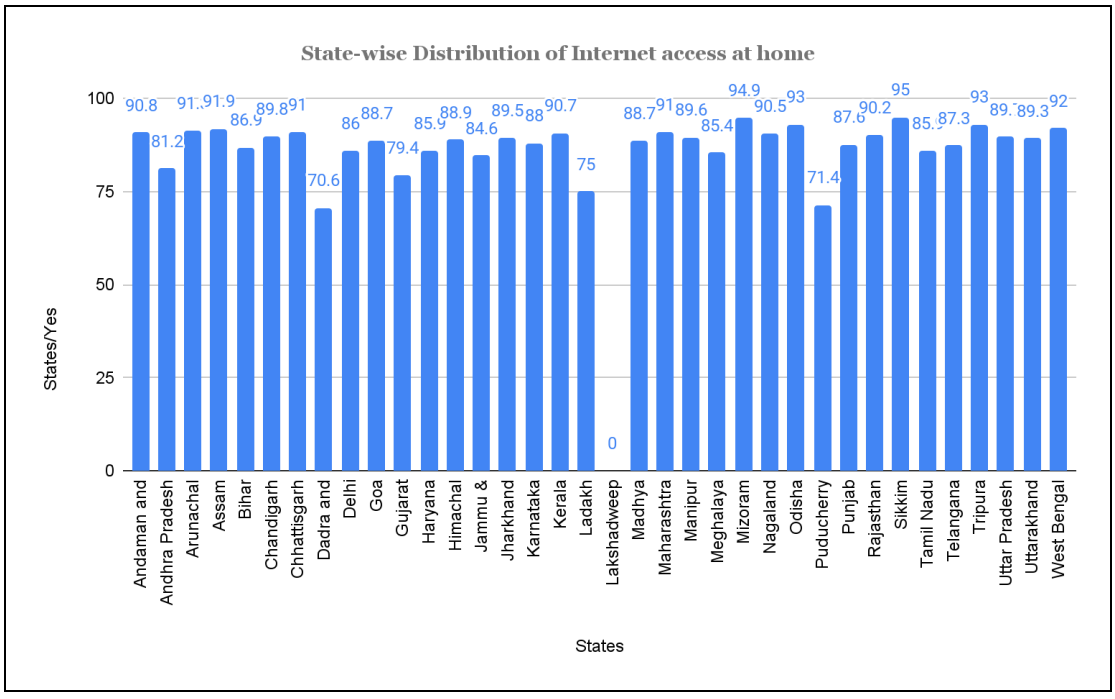


Fig 4.33: State-wise Distribution of Internet access at home

4.2.2.22: State-wise Distribution of Availability of personal email ID

Table 4.26: State-wise Distribution of Availability of personal email ID

States	E-Mail ID	Response (Number)	Response (Percentage)
Andaman and Nicobar Islands	No	50	28.9
	Yes	123	71.1
	Total	173	100.0
Andhra Pradesh	No	476	32.6
	Yes	985	67.4
	Total	1461	100.0
Arunachal Pradesh	No	43	17.8
	Yes	198	82.2
	Total	241	100.0
Assam	No	482	21.3
	Yes	1776	78.7
	Total	2258	100.0
Bihar	No	237	16.4
	Yes	1208	83.6
	Total	1445	100.0
Chandigarh	No	999	25.2
	Yes	2969	74.8
	Total	3968	100.0
Chhattisgarh	No	274	19.2
	Yes	1154	80.8
	Total	1428	100.0
Dadra and Nagar Haveli and Daman and Diu	No	11	32.4
	Yes	23	67.6
	Total	34	100.0
Delhi	No	11286	26.1
	Yes	31922	73.9
	Total	43208	100.0
Goa	No	665	19.3
	Yes	2784	80.7
	Total	3449	100.0
Gujarat	No	5	14.7
	Yes	29	85.3
	Total	34	100.0
Haryana	No	516	30.0
	Yes	1204	70.0
	Total	1720	100.0
Himachal Pradesh	No	1088	30.9
	Yes	2430	69.1

	Total	3518	100.0
Jammu & Kashmir	No	367	25.3
	Yes	1081	74.7
	Total	1448	100.0
Jharkhand	No	551	20.9
	Yes	2088	79.1
	Total	2639	100.0
Karnataka	No	283	22.9
	Yes	955	77.1
	Total	1238	100.0
Kerala	No	382	11.8
	Yes	2865	88.2
	Total	3247	100.0
Ladakh	No	2	16.7
	Yes	10	83.3
	Total	12	100.0
Lakshadweep	No	1	16.7
	Yes	5	83.3
	Total	6	100.0
Madhya Pradesh	No	516	18.1
	Yes	2339	81.9
	Total	2855	100.0
Maharashtra	No	873	23.3
	Yes	2876	76.7
	Total	3749	100.0
Manipur	No	53	32.3
	Yes	111	67.7
	Total	164	100.0
Meghalaya	No	25	26.0
	Yes	71	74.0
	Total	96	100.0
Mizoram	No	1686	31.5
	Yes	3664	68.5
	Total	5350	100.0
Nagaland	No	738	37.5
	Yes	1229	62.5
	Total	1967	100.0
Odisha	No	343	16.2
	Yes	1771	83.8
	Total	2114	100.0
Puducherry	No	4	57.1
	Yes	3	42.9
	Total	7	100.0

Punjab	No	4019	29.5
	Yes	9606	70.5
	Total	13625	100.0
Rajasthan	No	277	26.4
	Yes	773	73.6
	Total	1050	100.0
Sikkim	No	2	10.0
	Yes	18	90.0
	Total	20	100.0
Tamil Nadu	No	178	21.8
	Yes	637	78.2
	Total	815	100.0
Telangana	No	502	28.4
	Yes	1268	71.6
	Total	1770	100.0
Tripura	No	18	15.8
	Yes	96	84.2
	Total	114	100.0
Uttar Pradesh	No	1152	25.2
	Yes	3428	74.8
	Total	4580	100.0
Uttarakhand	No	519	24.4
	Yes	1612	75.6
	Total	2131	100.0
West Bengal	No	609	16.5
	Yes	3087	83.5
	Total	3696	100.0

From the above table 4.27, Mizoram has the highest percentage of students with personal email IDs at 68.5%. States like Delhi (73.9%) and Kerala (88.2%) also show a high prevalence of students with personal email IDs. On the other hand, states with relatively lower percentages include Dadra and Nagar Haveli and Daman and Diu (67.6%), Gujarat (85.3%), and Sikkim (90.0%). Conversely, states such as Uttar Pradesh (74.8%) and West Bengal (83.5%) also have significant percentages, though lower than the national average.

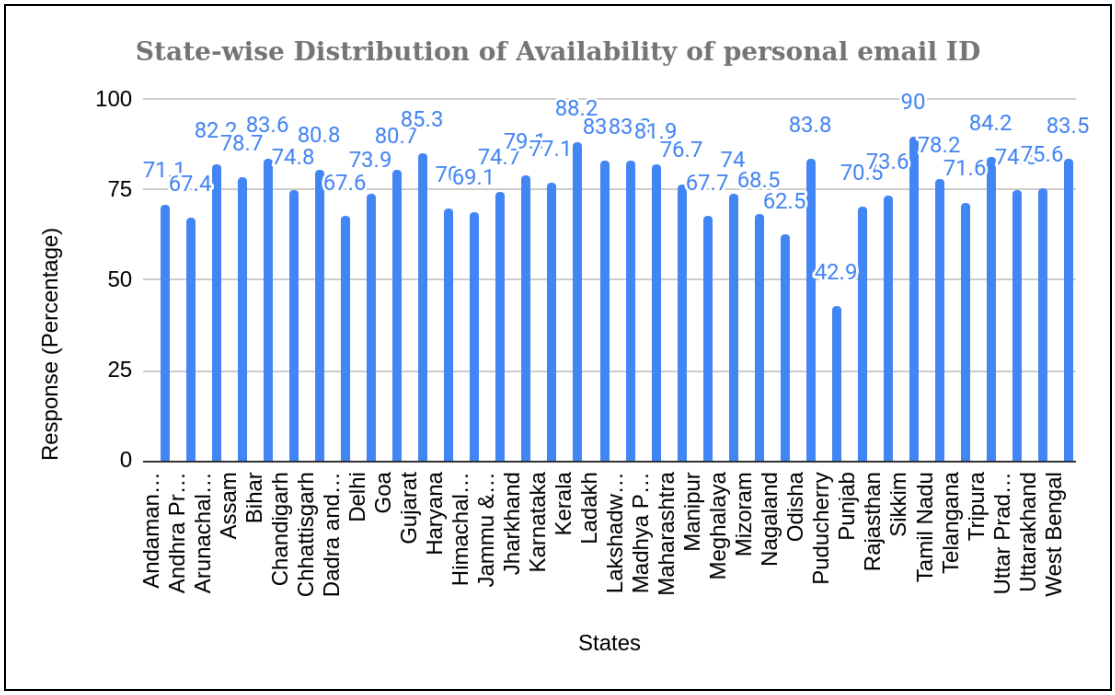


Fig 4.34: State-wise Distribution of Availability of personal email ID

4.2.2.23: State-wise Distribution of usage of digital devices per day

Table 4.27: State-wise Distribution of usage of digital devices per day

States	Usage of Digital devices per day	Response (Number)	Response (Percentage)
Andaman and Nicobar Islands	1 hour to 2 hours	49	28.3
	2 hours to 4 hours	15	8.7
	30 min to 1 hour	46	26.6
	Above 4 hours	5	2.9
	Do not use it everyday	7	4.0
	Less than 30 min	51	29.5
	Total	173	100.0
Andhra Pradesh	1 hour to 2 hours	330	22.6
	2 hours to 4 hours	186	12.7
	30 min to 1 hour	474	32.4
	Above 4 hours	51	3.5
	Do not use it everyday	117	8.0
	Less than 30 min	303	20.7
	Total	1461	100.0
Arunachal Pradesh	1 hour to 2 hours	74	30.7
	2 hours to 4 hours	44	18.3
	30 min to 1 hour	52	21.6
	Above 4 hours	27	11.2
	Do not use it everyday	12	5.0
	Less than 30 min	32	13.3

	Total	241	100.0
Assam	1 hour to 2 hours	641	28.4
	2 hours to 4 hours	378	16.7
	30 min to 1 hour	599	26.5
	Above 4 hours	189	8.4
	Do not use it everyday	158	7.0
	Less than 30 min	293	13.0
	Total	2258	100.0
Bihar	1 hour to 2 hours	360	24.9
	2 hours to 4 hours	226	15.6
	30 min to 1 hour	335	23.2
	Above 4 hours	149	10.3
	Do not use it everyday	105	7.3
	Less than 30 min	270	18.7
	Total	1445	100.0
Chandigarh	1 hour to 2 hours	1039	26.2
	2 hours to 4 hours	533	13.4
	30 min to 1 hour	1140	28.7
	Above 4 hours	198	5.0
	Do not use it everyday	294	7.4
	Less than 30 min	764	19.3
	Total	3968	100.0
Chhattisgarh	1 hour to 2 hours	465	32.6
	2 hours to 4 hours	232	16.2
	30 min to 1 hour	366	25.6
	Above 4 hours	118	8.3
	Do not use it everyday	60	4.2
	Less than 30 min	187	13.1
	Total	1428	100.0
Dadra and Nagar Haveli and Daman and Diu	2 hours to 4 hours	4	11.8
	30 min to 1 hour	9	26.5
	Above 4 hours	3	8.8
	Do not use it everyday	4	11.8
	Less than 30 min	14	41.2
	Total	34	100.0
Delhi	1 hour to 2 hours	11514	26.6
	2 hours to 4 hours	5356	12.4
	30 min to 1 hour	12347	28.6
	Above 4 hours	2575	6.0
	Do not use it everyday	3247	7.5
	Less than 30 min	8169	18.9
	Total	43208	100.0
Goa	1 hour to 2 hours	1002	29.1

	2 hours to 4 hours	614	17.8
	30 min to 1 hour	951	27.6
	Above 4 hours	280	8.1
	Do not use it everyday	186	5.4
	Less than 30 min	416	12.1
	Total	3449	100.0
Gujarat	1 hour to 2 hours	12	35.3
	2 hours to 4 hours	4	11.8
	30 min to 1 hour	7	20.6
	Do not use it everyday	1	2.9
	Less than 30 min	10	29.4
	Total	34	100.0
Haryana	1 hour to 2 hours	403	23.4
	2 hours to 4 hours	205	11.9
	30 min to 1 hour	514	29.9
	Above 4 hours	88	5.1
	Do not use it everyday	172	10.0
	Less than 30 min	338	19.7
	Total	1720	100.0
Himachal Pradesh	1 hour to 2 hours	757	21.5
	2 hours to 4 hours	303	8.6
	30 min to 1 hour	1159	32.9
	Above 4 hours	122	3.5
	Do not use it everyday	311	8.8
	Less than 30 min	866	24.6
	Total	3518	100.0
Jammu & Kashmir	1 hour to 2 hours	379	26.2
	2 hours to 4 hours	157	10.8
	30 min to 1 hour	406	28.0
	Above 4 hours	79	5.5
	Do not use it everyday	117	8.1
	Less than 30 min	310	21.4
	Total	1448	100.0
Jharkhand	1 hour to 2 hours	730	27.7
	2 hours to 4 hours	345	13.1
	30 min to 1 hour	759	28.8
	Above 4 hours	170	6.4
	Do not use it everyday	179	6.8
	Less than 30 min	456	17.3
	Total	2639	100.0
Karnataka	1 hour to 2 hours	339	27.4
	2 hours to 4 hours	202	16.3
	30 min to 1 hour	354	28.6

	Above 4 hours	67	5.4
	Do not use it everyday	85	6.9
	Less than 30 min	191	15.4
	Total	1238	100.0
Kerala	1 hour to 2 hours	986	30.4
	2 hours to 4 hours	587	18.1
	30 min to 1 hour	926	28.5
	Above 4 hours	195	6.0
	Do not use it everyday	204	6.3
	Less than 30 min	349	10.7
	Total	3247	100.0
Ladakh	1 hour to 2 hours	2	16.7
	30 min to 1 hour	6	50.0
	Do not use it everyday	1	8.3
	Less than 30 min	3	25.0
	Total	12	100.0
Lakshadweep	1 hour to 2 hours	2	33.3
	30 min to 1 hour	1	16.7
	Do not use it everyday	1	16.7
	Less than 30 min	2	33.3
	Total	6	100.0
Madhya Pradesh	1 hour to 2 hours	729	25.5
	2 hours to 4 hours	390	13.7
	30 min to 1 hour	888	31.1
	Above 4 hours	185	6.5
	Do not use it everyday	170	6.0
	Less than 30 min	493	17.3
	Total	2855	100.0
Maharashtra	1 hour to 2 hours	1098	29.3
	2 hours to 4 hours	631	16.8
	30 min to 1 hour	1044	27.8
	Above 4 hours	230	6.1
	Do not use it everyday	196	5.2
	Less than 30 min	550	14.7
	Total	3749	100.0
Manipur	1 hour to 2 hours	40	24.4
	2 hours to 4 hours	30	18.3
	30 min to 1 hour	42	25.6
	Above 4 hours	20	12.2
	Do not use it everyday	20	12.2
	Less than 30 min	12	7.3
	Total	164	100.0
Meghalaya	1 hour to 2 hours	28	29.2

	2 hours to 4 hours	14	14.6
	30 min to 1 hour	29	30.2
	Above 4 hours	5	5.2
	Do not use it everyday	9	9.4
	Less than 30 min	11	11.5
	Total	96	100.0
Mizoram	1 hour to 2 hours	1632	30.5
	2 hours to 4 hours	1142	21.3
	30 min to 1 hour	1203	22.5
	Above 4 hours	486	9.1
	Do not use it everyday	379	7.1
	Less than 30 min	508	9.5
	Total	5350	100.0
Nagaland	1 hour to 2 hours	482	24.5
	2 hours to 4 hours	329	16.7
	30 min to 1 hour	476	24.2
	Above 4 hours	99	5.0
	Do not use it everyday	332	16.9
	Less than 30 min	249	12.7
	Total	1967	100.0
Odisha	1 hour to 2 hours	647	30.6
	2 hours to 4 hours	478	22.6
	30 min to 1 hour	517	24.5
	Above 4 hours	209	9.9
	Do not use it everyday	97	4.6
	Less than 30 min	166	7.9
	Total	2114	100.0
Puducherry	1 hour to 2 hours	1	14.3
	30 min to 1 hour	1	14.3
	Do not use it everyday	3	42.9
	Less than 30 min	2	28.6
	Total	7	100.0
Punjab	1 hour to 2 hours	2983	21.9
	2 hours to 4 hours	1068	7.8
	30 min to 1 hour	4260	31.3
	Above 4 hours	547	4.0
	Do not use it everyday	1060	7.8
	Less than 30 min	3707	27.2
	Total	13625	100.0
Rajasthan	1 hour to 2 hours	248	23.6
	2 hours to 4 hours	131	12.5
	30 min to 1 hour	344	32.8
	Above 4 hours	53	5.0

	Do not use it everyday	90	8.6
	Less than 30 min	184	17.5
	Total	1050	100.0
Sikkim	1 hour to 2 hours	5	25.0
	2 hours to 4 hours	5	25.0
	30 min to 1 hour	3	15.0
	Above 4 hours	1	5.0
	Do not use it everyday	1	5.0
	Less than 30 min	5	25.0
	Total	20	100.0
Tamil Nadu	1 hour to 2 hours	207	25.4
	2 hours to 4 hours	124	15.2
	30 min to 1 hour	246	30.2
	Above 4 hours	47	5.8
	Do not use it everyday	62	7.6
	Less than 30 min	129	15.8
	Total	815	100.0
Telangana	1 hour to 2 hours	518	29.3
	2 hours to 4 hours	203	11.5
	30 min to 1 hour	580	32.8
	Above 4 hours	98	5.5
	Do not use it everyday	91	5.1
	Less than 30 min	280	15.8
	Total	1770	100.0
Tripura	1 hour to 2 hours	32	28.1
	2 hours to 4 hours	25	21.9
	30 min to 1 hour	24	21.1
	Above 4 hours	16	14.0
	Do not use it everyday	11	9.6
	Less than 30 min	6	5.3
	Total	114	100.0
Uttar Pradesh	1 hour to 2 hours	1316	28.7
	2 hours to 4 hours	619	13.5
	30 min to 1 hour	1298	28.3
	Above 4 hours	330	7.2
	Do not use it everyday	338	7.4
	Less than 30 min	679	14.8
	Total	4580	100.0
Uttarakhand	1 hour to 2 hours	546	25.6
	2 hours to 4 hours	231	10.8
	30 min to 1 hour	644	30.2
	Above 4 hours	95	4.5
	Do not use it everyday	210	9.9

	Less than 30 min	405	19.0
	Total	2131	100.0
West Bengal	1 hour to 2 hours	1147	31.0
	2 hours to 4 hours	658	17.8
	30 min to 1 hour	1021	27.6
	Above 4 hours	294	8.0
	Do not use it everyday	222	6.0
	Less than 30 min	354	9.6
	Total	3696	100.0

From the above table 4.27, the Majority of students (29.5%) from Andaman and Nicobar Islands use digital devices for less than 30 minutes daily. It was found that the majority of students (32.4%) from Andhra Pradesh use digital devices for 30 minutes to 1 hour daily, and the majority of students (30.7%) from Arunachal Pradesh use digital devices for 1 hour to 2 hours daily. Across different states, usage patterns vary, with the highest percentages seen in shorter durations like 30 minutes to 1 hour and 1 hour to 2 hours daily, while fewer students use digital devices for more than 4 hours or do not use them every day.

4.2.2.24: State-wise Distribution of consideration of hours as excessive screen time

Table 4.28: State-wise Distribution of consideration of hours as excessive screen time

States	Excessive Screen Time	Response (Number)	Response (Percentage)
Andaman and Nicobar Islands	1 hour to 2 hours	40	23.1
	2 hours to 4 hours	19	11.0
	30 min to 1 hour	33	19.1
	More than 4 hours	18	10.4
	Upto 30 min	63	36.4
	Total	173	100.0
Andhra Pradesh	1 hour to 2 hours	243	16.6
	2 hours to 4 hours	183	12.5
	30 min to 1 hour	364	24.9
	More than 4 hours	149	10.2
	Upto 30 min	522	35.7
	Total	1461	100.0
Arunachal Pradesh	1 hour to 2 hours	51	21.2
	2 hours to 4 hours	31	12.9
	30 min to 1 hour	60	24.9
	More than 4 hours	44	18.3
	Upto 30 min	55	22.8
	Total	241	100.0
Assam	1 hour to 2 hours	415	18.4
	2 hours to 4 hours	425	18.8
	30 min to 1 hour	419	18.6
	More than 4 hours	432	19.1

	Upto 30 min	567	25.1
	Total	2258	100.0
Bihar	1 hour to 2 hours	289	20.0
	2 hours to 4 hours	214	14.8
	30 min to 1 hour	299	20.7
	More than 4 hours	210	14.5
	Upto 30 min	433	30.0
	Total	1445	100.0
Chandigarh	1 hour to 2 hours	699	17.6
	2 hours to 4 hours	686	17.3
	30 min to 1 hour	800	20.2
	More than 4 hours	699	17.6
	Upto 30 min	1084	27.3
	Total	3968	100.0
Chhattisgarh	1 hour to 2 hours	328	23.0
	2 hours to 4 hours	251	17.6
	30 min to 1 hour	303	21.2
	More than 4 hours	225	15.8
	Upto 30 min	321	22.5
	Total	1428	100.0
Dadra and Nagar Haveli and Daman and Diu	1 hour to 2 hours	1	2.9
	2 hours to 4 hours	5	14.7
	30 min to 1 hour	4	11.8
	More than 4 hours	4	11.8
	Upto 30 min	20	58.8
	Total	34	100.0
Delhi	1 hour to 2 hours	8657	20.0
	2 hours to 4 hours	5682	13.2
	30 min to 1 hour	10673	24.7
	More than 4 hours	5236	12.1
	Upto 30 min	12960	30.0
	Total	43208	100.0
Goa	1 hour to 2 hours	641	18.6
	2 hours to 4 hours	565	16.4
	30 min to 1 hour	755	21.9
	More than 4 hours	700	20.3
	Upto 30 min	788	22.8
	Total	3449	100.0
Gujarat	1 hour to 2 hours	4	11.8
	2 hours to 4 hours	8	23.5
	30 min to 1 hour	10	29.4
	More than 4 hours	4	11.8
	Upto 30 min	8	23.5

	Total	34	100.0
Haryana	1 hour to 2 hours	348	20.2
	2 hours to 4 hours	203	11.8
	30 min to 1 hour	416	24.2
	More than 4 hours	212	12.3
	Upto 30 min	541	31.5
	Total	1720	100.0
Himachal Pradesh	1 hour to 2 hours	639	18.2
	2 hours to 4 hours	364	10.3
	30 min to 1 hour	894	25.4
	More than 4 hours	301	8.6
	Upto 30 min	1320	37.5
	Total	3518	100.0
Jammu & Kashmir	1 hour to 2 hours	289	20.0
	2 hours to 4 hours	176	12.2
	30 min to 1 hour	366	25.3
	More than 4 hours	149	10.3
	Upto 30 min	468	32.3
	Total	1448	100.0
Jharkhand	1 hour to 2 hours	535	20.3
	2 hours to 4 hours	363	13.8
	30 min to 1 hour	670	25.4
	More than 4 hours	303	11.5
	Upto 30 min	768	29.1
	Total	2639	100.0
Karnataka	1 hour to 2 hours	257	20.8
	2 hours to 4 hours	193	15.6
	30 min to 1 hour	244	19.7
	More than 4 hours	227	18.3
	Upto 30 min	317	25.6
	Total	1238	100.0
Kerala	1 hour to 2 hours	667	20.5
	2 hours to 4 hours	684	21.1
	30 min to 1 hour	657	20.2
	More than 4 hours	736	22.7
	Upto 30 min	503	15.5
	Total	3247	100.0
Ladakh	1 hour to 2 hours	1	8.3
	30 min to 1 hour	5	41.7
	More than 4 hours	1	8.3
	Upto 30 min	5	41.7
	Total	12	100.0
Lakshadweep	1 hour to 2 hours	1	16.7

	30 min to 1 hour	1	16.7
	Upto 30 min	4	66.7
	Total	6	100.0
Madhya Pradesh	1 hour to 2 hours	601	21.1
	2 hours to 4 hours	404	14.2
	30 min to 1 hour	712	24.9
	More than 4 hours	342	12.0
	Upto 30 min	796	27.9
	Total	2855	100.0
Maharashtra	1 hour to 2 hours	824	22.0
	2 hours to 4 hours	716	19.1
	30 min to 1 hour	732	19.5
	More than 4 hours	616	16.4
	Upto 30 min	861	23.0
	Total	3749	100.0
Manipur	1 hour to 2 hours	27	16.5
	2 hours to 4 hours	23	14.0
	30 min to 1 hour	41	25.0
	More than 4 hours	39	23.8
	Upto 30 min	34	20.7
	Total	164	100.0
Meghalaya	1 hour to 2 hours	20	20.8
	2 hours to 4 hours	17	17.7
	30 min to 1 hour	33	34.4
	More than 4 hours	12	12.5
	Upto 30 min	14	14.6
	Total	96	100.0
Mizoram	1 hour to 2 hours	1209	22.6
	2 hours to 4 hours	870	16.3
	30 min to 1 hour	1312	24.5
	More than 4 hours	943	17.6
	Upto 30 min	1016	19.0
	Total	5350	100.0
Nagaland	1 hour to 2 hours	375	19.1
	2 hours to 4 hours	269	13.7
	30 min to 1 hour	498	25.3
	More than 4 hours	277	14.1
	Upto 30 min	548	27.9
	Total	1967	100.0
Odisha	1 hour to 2 hours	460	21.8
	2 hours to 4 hours	493	23.3
	30 min to 1 hour	337	15.9
	More than 4 hours	449	21.2

	Upto 30 min	375	17.7
	Total	2114	100.0
Puducherry	2 hours to 4 hours	1	14.3
	30 min to 1 hour	1	14.3
	Upto 30 min	5	71.4
	Total	7	100.0
Punjab	1 hour to 2 hours	2357	17.3
	2 hours to 4 hours	1195	8.8
	30 min to 1 hour	3627	26.6
	More than 4 hours	890	6.5
	Upto 30 min	5556	40.8
	Total	13625	100.0
Rajasthan	1 hour to 2 hours	220	21.0
	2 hours to 4 hours	155	14.8
	30 min to 1 hour	273	26.0
	More than 4 hours	128	12.2
	Upto 30 min	274	26.1
	Total	1050	100.0
Sikkim	1 hour to 2 hours	3	15.0
	2 hours to 4 hours	3	15.0
	30 min to 1 hour	5	25.0
	More than 4 hours	4	20.0
	Upto 30 min	5	25.0
	Total	20	100.0
Tamil Nadu	1 hour to 2 hours	167	20.5
	2 hours to 4 hours	141	17.3
	30 min to 1 hour	174	21.3
	More than 4 hours	124	15.2
	Upto 30 min	209	25.6
	Total	815	100.0
Telangana	1 hour to 2 hours	364	20.6
	2 hours to 4 hours	309	17.5
	30 min to 1 hour	405	22.9
	More than 4 hours	222	12.5
	Upto 30 min	470	26.6
	Total	1770	100.0
Tripura	1 hour to 2 hours	27	23.7
	2 hours to 4 hours	14	12.3
	30 min to 1 hour	19	16.7
	More than 4 hours	34	29.8
	Upto 30 min	20	17.5
	Total	114	100.0
Uttar Pradesh	1 hour to 2 hours	969	21.2

	2 hours to 4 hours	688	15.0
	30 min to 1 hour	1113	24.3
	More than 4 hours	562	12.3
	Upto 30 min	1248	27.2
	Total	4580	100.0
Uttarakhand	1 hour to 2 hours	402	18.9
	2 hours to 4 hours	277	13.0
	30 min to 1 hour	563	26.4
	More than 4 hours	254	11.9
	Upto 30 min	635	29.8
	Total	2131	100.0
West Bengal	1 hour to 2 hours	780	21.1
	2 hours to 4 hours	781	21.1
	30 min to 1 hour	650	17.6
	More than 4 hours	789	21.3
	Upto 30 min	696	18.8
	Total	3696	100.0

From the above table 4.28, the Majority of students from Arunachal Pradesh (21.2%) and Gujarat (11.8%) consider 1 hour to 2 hours as excessive screen time. States like Odisha (23.3%) and Kerala (21.1%) have the majority considering 2 hours to 4 hours as excessive screen time. In Mizoram (24.5%) and Haryana (24.2%), the majority of students consider 30 minutes to 1 hour as excessive screen time. Only a small number of states indicated any significant proportion of students who do not use digital devices every day. Majority of students from most states, including Andaman and Nicobar Islands (36.4%), Andhra Pradesh (35.7%), and Delhi (30.0%), consider up to 30 minutes as excessive screen time. In contrast, in states like Kerala (22.7%) and West Bengal (21.3%), the majority of students consider more than 4 hours as excessive screen time. Here are the states where the majority of students indicated not using digital devices every day:

- Dadra and Nagar Haveli and Daman and Diu: 58.8%
- Puducherry: 71.4%
- Lakshadweep: 66.7%

4.2.2.25: State-wise Distribution of courses related to ICT

Table 4.29: State-wise Distribution of courses related to ICT

States	ICT	Response (Number)	Response (Percentage)
Andaman and Nicobar Islands	No	68	39.3
	Yes	105	60.7
	Total	173	100.0

Andhra Pradesh	No	816	55.9
	Yes	645	44.1
	Total	1461	100.0
Arunachal Pradesh	No	133	55.2
	Yes	108	44.8
	Total	241	100.0
Assam	No	1429	63.3
	Yes	829	36.7
	Total	2258	100.0
Bihar	No	726	50.2
	Yes	719	49.8
	Total	1445	100.0
Chandigarh	No	1948	49.1
	Yes	2020	50.9
	Total	3968	100.0
Chhattisgarh	No	831	58.2
	Yes	597	41.8
	Total	1428	100.0
Dadra and Nagar Haveli and Daman and Diu	No	14	41.2
	Yes	20	58.8
	Total	34	100.0
Delhi	No	21368	49.5
	Yes	21840	50.5
	Total	43208	100.0
Goa	No	2111	61.2
	Yes	1338	38.8
	Total	3449	100.0
Gujarat	No	20	58.8

	Yes	14	41.2
	Total	34	100.0
Haryana	No	916	53.3
	Yes	804	46.7
	Total	1720	100.0
Himachal Pradesh	No	1499	42.6
	Yes	2019	57.4
	Total	3518	100.0
Jammu & Kashmir	No	831	57.4
	Yes	617	42.6
	Total	1448	100.0
Jharkhand	No	1330	50.4
	Yes	1309	49.6
	Total	2639	100.0
Karnataka	No	767	62.0
	Yes	471	38.0
	Total	1238	100.0
Kerala	No	2181	67.2
	Yes	1066	32.8
	Total	3247	100.0
Ladakh	No	4	33.3
	Yes	8	66.7
	Total	12	100.0
Lakshadweep	No	1	16.7
	Yes	5	83.3
	Total	6	100.0
Madhya Pradesh	No	1622	56.8
	Yes	1233	43.2

	Total	2855	100.0
Maharashtra	No	2357	62.9
	Yes	1392	37.1
	Total	3749	100.0
Manipur	No	116	70.7
	Yes	48	29.3
	Total	164	100.0
Meghalaya	No	53	55.2
	Yes	43	44.8
	Total	96	100.0
Mizoram	No	3215	60.1
	Yes	2135	39.9
	Total	5350	100.0
Nagaland	No	1086	55.2
	Yes	881	44.8
	Total	1967	100.0
Odisha	No	1093	51.7
	Yes	1021	48.3
	Total	2114	100.0
Puducherry	No	5	71.4
	Yes	2	28.6
	Total	7	100.0
Punjab	No	5425	39.8
	Yes	8200	60.2
	Total	13625	100.0
Rajasthan	No	590	56.2
	Yes	460	43.8
	Total	1050	100.0

Sikkim	No	11	55.0
	Yes	9	45.0
	Total	20	100.0
Tamil Nadu	No	584	71.7
	Yes	231	28.3
	Total	815	100.0
Telangana	No	1086	61.4
	Yes	684	38.6
	Total	1770	100.0
Tripura	No	72	63.2
	Yes	42	36.8
	Total	114	100.0
Uttar Pradesh	No	2590	56.6
	Yes	1990	43.4
	Total	4580	100.0
Uttarakhand	No	1156	54.2
	Yes	975	45.8
	Total	2131	100.0
West Bengal	No	2534	68.6
	Yes	1162	31.4
	Total	3696	100.0

From the above table 4.29 ,the majority of students (60.7%) from Andaman and Nicobar Islands use ICT. In Delhi, 50.5% of students use ICT. In Punjab, 60.2% of students use ICT. The majority of students (57.4%) from Himachal Pradesh use ICT. In Ladakh, 66.7% of students use ICT. The majority of students (83.3%) from Lakshadweep use ICT.

4.2.3 Analysis of Data with Regard to Awareness About Cyber Safety and Security

This section outlines the data analysis of the CSSA scale with regard to the selected sub groups. For the analysis of data, several hypotheses were proposed and the data was analyzed to answer each proposed hypothesis. The results of data analysis have been presented in the following sections under different headings. Mainly the overall score of CSSA scale was used for data

analysis and wherever possible, the various dimensions of CSSA scale was also taken into consideration to get a better insight into the nature of understanding about CSSA among secondary students.

4.2.3.1 Analysis of overall score of CSSA with regard to exposure to ICT

In this section, the significant difference of overall score of CSSA against various sub-groups of students with regard to their exposure to various aspects of ICT/ digital devices was studied. For the analysis of data, the following hypotheses were proposed:

There is no significant difference in the mean score of cyber safety and security awareness of secondary students with respect to their/the

1. Access to internet at home
2. Possession of personal email ID
3. Participation in ICT courses
4. Availability of digital devices at home
5. Availability of own digital devices
6. Possession of personal social media account
7. Duration of use of devices per day
8. Perception about excessive screen time

Each hypothesis were taken separately and the analysis was performed and is given in the following sections:

4.2.3.1.1 Analysis of overall score of CSSA with regard access to internet at home

To study the effect of internet access at home on the overall CSSA of secondary students, a null hypothesis "There is no significant difference in the mean score of cyber safety and security awareness of secondary students with respect to their access to internet at home" has been proposed. t test was performed to analyze the data and the results are given in the following table:

Table 4.30: Cyber Safety and Security Awareness (CSSA) with respect to access to internet at home

	Internet at home	N	Mean	Std. Deviation	t	Sig. (2-tailed)
Total Awareness Score	No	13717	182.36	29.31	-39.14	.000
	Yes	101914	193.47	31.46		

From Table 4.30 it is evident that the obtained t value **-39.14** is significant at 0.01 level ($p<0.01$). This means that there is a significant difference in the mean scores of awareness about cyber safety and security among students who have and who haven't have access to the internet at home and hence the null hypothesis, that is, There is no significant difference in the mean score of cyber safety and security awareness of secondary students with respect to Their access to internet at home is **not accepted** and the alternate hypothesis is upheld. Further, from the mean scores, it is evident that those students with internet access at home have a higher

mean score (193.47) compared to those without it (182.36). Students with internet access at home tend to have a higher average awareness score compared to those without internet access.

4.2.3.1.2 Analysis of overall score of CSSA with regard to having personal email ID

To study the effect of having personal email ID on the overall CSSA of secondary students, a null hypothesis that there is no significant difference in the mean score of cyber safety and security awareness of secondary students with respect to their possession of personal email ID has been proposed. t test was performed to analyze the data and the results are given in the following table:

Table 4.31: CSSA with respect to availability of personal Email ID

	Own Email ID	N	Mean	Std. Deviation	t	Sig. (2-tailed)
Total Awareness Score	No	29232	190.54	30.80	-10.13	.000
	Yes	86399	192.70	31.60		

From Table 4.31 it is evident that the obtained t value **-10.13** is significant at 0.01 level($p<0.01$). This means that there is a significant difference in the mean scores of awareness about cyber safety and security among students who have their email IDs to the ones who didn't and hence the null hypothesis, that is, **"**There is no significant difference in the mean score of cyber safety and security awareness of secondary students with respect to Their possession of personal email ID" is **not accepted** and the alternate hypothesis is upheld. Further, from the mean scores, it is evident that those students who have their email ID have a slightly higher mean total awareness score (192.70) as compared to those who do not have their email ID (190.54).

4.2.3.1.3 Analysis of overall score of CSSA with regard to participation in ICT courses.

To study the effect of participation in ICT courses on the overall CSSA of secondary students, a null hypothesis, there is no significant difference in the total awareness scores between students who have participated in ICT courses and those who have not has been proposed. t test was performed to analyze the data and the results are given in the following table:

Table 4.32: CSSA with respect to ICT Course Participation

	ICT course	N	Mean	Std. Deviation	t	Sig. (2-tailed)
Total Awareness Score	No	60588	194.52	30.45	26.97	.000
	Yes	55043	189.55	32.25		

From Table 4.32 it is evident that the obtained t value **26.97** is significant at 0.01 level($p<0.01$). This means that there is a significant difference in the mean scores of awareness about cyber safety and security among students who participated in the ICT course and who didn't, hence the null hypothesis, that is, **there is no significant difference in the total awareness scores between students who have participated in ICT courses and those who**

have not and is **not accepted** and the alternate hypothesis is upheld. Further, from the mean scores, it is evident that the students who have not participated in ICT courses have a higher average total awareness score (194.52) compared to those who have participated (189.55).

4.2.3.1.4 Analysis of overall score of CSSA with regard to Access the Digital Devices at Home.

To study the effect of access to digital devices at home on the overall CSSA of secondary students, a null hypothesis, there is no significant difference in the total awareness scores between individuals who have access to digital devices at home and those who do not has been proposed. t test was performed to analyze the data and the results are given in the following table:

Table 4.33: CSSA with respect to Access To Digital Gadgets at Home

	Availability of devices at home	N	Mean	Std. Deviation	t	Sig. (2-tailed)
Total Awareness Score	No	1198	173.51	26.29	-20.68	.000
	Yes	114433	192.35	31.41		

From Table 4.33 it is evident that the obtained t value **-20.68** is significant at 0.01 level($p<0.01$). This means that there is a significant difference in the mean scores of awareness about cyber safety and security among students who have access to digital devices at home and those who didn't, hence the null hypothesis, that is, **there is no significant difference in the total awareness scores between individuals who have access to digital devices at home and those who do not** is **not accepted** and the alternate hypothesis is upheld. Further, from the mean scores, it is evident that the students who have access to digital devices at home have a higher average total awareness score (192.35) compared to those who haven't (173.51).

4.2.3.1.5 Analysis of overall score of CSSA with regard to availability of own digital devices.

To study the effect of availability of own digital devices on the overall CSSA of secondary students, a null hypothesis, there is no significant difference in the total awareness scores between individuals who use their devices and those who do not has been proposed. t test was performed to analyze the data and the results are given in the following table:

Table 4.34: CSSA with respect to Availability Of Own Digital Gadgets

	Using own device	N	Mean	Std. Deviation	t	Sig. (2-tailed)
Total Awareness Score	No	18962	195.88	30.35	17.89	.000
	Yes	96669	191.42	31.57		

From Table 4.34 it is evident that the obtained t value **17.89** is significant at 0.01 level($p<0.01$). This means that there is a significant difference in the mean scores of awareness

about cyber safety and security among students who have availability of their device to the ones who don't, hence the null hypothesis, that is, **there is no significant difference in the total awareness scores between individuals who use their device and those who do not** is **not accepted** and the alternate hypothesis is upheld. Further, from the mean scores, it is evident that the students who don't have availability of their devices have a higher average total awareness score (195.88) compared to those who have (191.42).

4.2.3.1.6 Analysis of overall score of CSSA with regard to having a social media account.

To study the effect of having a social media account on the overall CSSA of secondary students, a null hypothesis, There is no significant difference in the total awareness scores between individuals who have a social media account and those who do not has been proposed. t test was performed to analyze the data and the results are given in the following table:

Table 4.35: CSSA with respect to having Social Media Account

	Social Media Account	N	Mean	Std. Deviation	t	Sig. (2-tailed)
Total Awareness Score	No	36423	194.92	31.89	20.34	.000
	Yes	79208	190.88	31.11		

From Table 4.35 it is evident that the obtained t value **20.34** is significant at 0.01 level($p<0.01$). This means that there is a significant difference in the mean scores of awareness about cyber safety and security among students who have their social media accounts to the ones who don't, hence the null hypothesis, that is, **there is no significant difference in the total awareness scores between individuals who have a social media account and those who do not** is **not accepted** and the alternate hypothesis is upheld. Further, from the mean scores, it is evident that the students who don't have availability of their social media account have a higher average total awareness score (194.92) compared to those who have (190.88).

4.2.3.1.7 Analysis of overall score of CSSA with regard to duration of use of digital devices.

Table 4.36 CSSA with respect to duration of use of digital devices

	Sum of Squares	Df	Mean Square	F	Sig.
Between Groups	5240428.62	5	1048085.72	1112.69	.000
Within Groups	108911048.71	115625	941.93		
Total	114151477.33	115630			

The obtained F value is 1112.69, which is significant at 0.01 level ($p<0.01$). This means that there exists a significant difference in Cyber Security and Safety awareness with regard to the duration of use of digital devices per day. Hence, the null hypothesis stating that there is no significant difference in cyber security awareness among students using digital devices for varying durations in a day has not been accepted and the alternate hypothesis is upheld. In order

to find out differences among groups, Duncan's post-hoc test has been performed and the results are given in the following table.

POST HOC

Table 4.37 CSSA post hos analysis with respect to duration of use of digital devices

Duncan[a,b] Subset for alpha = 0.05

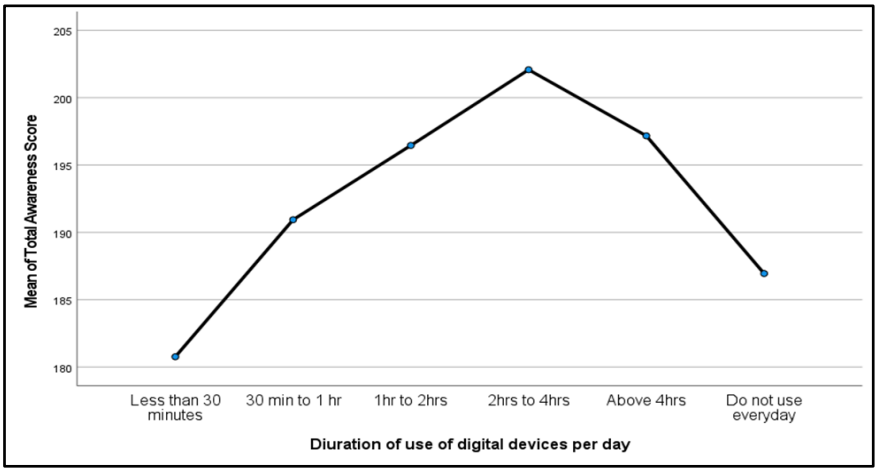
Duration of use of digital devices per day	N	1	2	3	4	5
Less than 30 minutes	20764	180.77				
Do not use everyday	8552		186.95			
30 min to 1 hr.	33071			190.94		
1hr to 2hrs	30744				196.46	
Above 4hrs	7031				197.17	
2hrs to 4hrs	15469					202.07
Sig.		1.000	1.000	1.000	.055	1.000

Means for groups in homogeneous subsets are displayed.

a. Uses Harmonic Mean Sample Size = 13801.69.

b. The group sizes are unequal. The harmonic mean of the group sizes is used. Type I error levels are not guaranteed.

From the above table, it is clear that the mean awareness scores of students using digital devices daily varies across the groups. The obtained mean score of those students using digital devices for 2-4 hrs. (202.07) was found to be greater among all the groups and the smallest mean score was observed among students using digital devices for less than 30 minutes (180.77). Hence it can be concluded that the students are using digital devices for 2-4 hrs. are having higher levels of awareness about cyber safety and security. The mean scores are plotted in the mean plot below.



4.2.3.1.8 Analysis of overall score of CSSA with regard to excessive screen time.

Table 4.39 CSSA with respect to Excessive Screen Time

	Sum of Squares	Df	Mean Square	F	Sig.
Between Groups	10743720.41	4	2685930.10	3003.28	.000
Within Groups	103407756.92	115626	894.33		
Total	114151477.33	115630			

The obtained F value is 3003.28, which is significant at 0.01 level ($p<0.01$). This means that there exists a significant difference in Cyber Security and Safety awareness with regard to their perception about excessive screen time. Hence, the null hypothesis stating that there is no significant difference in cyber security awareness among students with respect to Their perception about excessive screen time has not been accepted and the alternate hypothesis is upheld. In order to find out differences among groups, Duncan's post-hoc test has been performed and the results are given in the following table.

POST HOC

Table 4.40 CSSA post hoc analysis with respect to excessive screen time

Duncan[a,b] Subset for alpha = 0.05

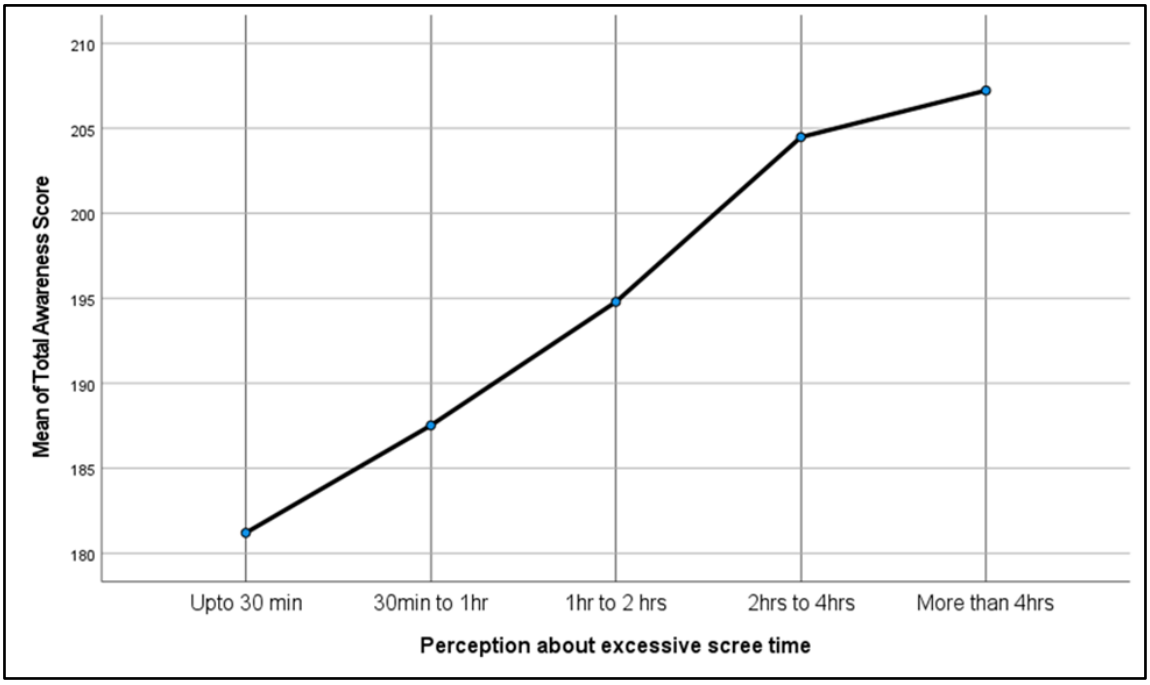
Duration of use of digital devices per day	N	1	2	3	4	5
Upto 30 min	33509	181.21				
30 min to 1 hr.	27469		187.53			
1hr to 2hrs	22910			194.79		
2hrs to 4hrs	16408				204.49	
More than 4hrs	15335					207.23
Sig.		1.000	1.000	1.000	1.000	1.000

Means for groups in homogeneous subsets are displayed.

a. Uses Harmonic Mean Sample Size = 21181.715.
b. The group sizes are unequal. The harmonic mean of the group sizes is used. Type I error levels are not guaranteed.

From the above table, it is clear that the mean awareness scores of students using digital devices daily varies across the groups. The obtained mean score of those students who perceive use of digital gadgets for more than 4 hrs (207.23) as excessive screen time was found to be greater among all the groups and the smallest mean score was observed among students who perceive use of digital gadgets for up to 30 minutes (181.21) as excessive. Hence it can be concluded that the students who perceive excessive screen time as more than 4 hrs are having

higher levels of awareness about cyber safety and security. The mean scores are plotted in the mean plot below.



4.2.3.2 Analysis of overall score of CSSA with regard to demographic variables

In this section, the significant difference of overall score of CSSA against various sub-groups of demographic factors of students was studied. The data has been analyzed by considering the overall score of CSSA as well as dimension-wise scores of CSSA. For the analysis of data, the following two broader hypotheses were proposed:

There is no significant difference in the mean scores of cyber safety and security awareness of secondary students with respect to

1. Locale of the school
2. Gender of the student
3. Standard in which the students are studying
4. Type of school

There is no significant difference in the mean score of different dimensions of cyber safety and security awareness of secondary students with respect to

1. Locale of the school
2. Gender of the student
3. Standard in which the students are studying
4. Type of school

4.2.3.2.1 Analysis of effect of locale of the school on overall and dimension wise scores of CSSA

To study the effect of the locale of the school on the overall CSSA of secondary students, a null hypothesis “There is no significant difference in the mean score of cyber safety and security awareness of secondary students with respect to the locale of the school” has been proposed. Further, to analyze the effect of locale of the school on various dimensions of CSSA,

another hypothesis “There is no significant difference in the mean score of different dimensions of cyber safety and security awareness of secondary students with respect to locale of the school” was also proposed. t test was performed to analyze the data and the results are given in the following table:

Table 4.44 Locality and their dimensions scores

	Locale	N	Mean	Std. Deviation	t	Sig. (2-tailed)
Total Awareness Score	**Rural**	36467	184.12	29.98	-59.91	.000
	Urban	79163	195.85	31.37		
Psychological Dimension	**Rural**	36467	36.13	13.81	-48.79	.000
	Urban	79163	40.15	12.63		
Physical Dimension	**Rural**	36467	34.57	5.73	-50.71	.000
	Urban	79163	36.45	5.89		
Legal Dimension	**Rural**	36467	32.50	4.71	-47.06	.000
	Urban	79163	34.05	5.37		
Socio-Ethical Dimension	**Rural**	36467	42.06	6.55	-51.25	.000
	Urban	79163	44.41	7.50		
Technical Dimension	**Rural**	36467	38.84	5.48	-49.66	.000
	Urban	79163	40.80	6.52		

There is a significant difference in the mean score of secondary students about their awareness about cyber safety and security (CSS) with regard to their locale. The difference is significant across all the dimensions of CSS.

From the above table, it is evident that the obtained t value of 59.91 is significant at 0.05 level. This means that there is a significant difference in the mean scores of awareness about cyber safety and security among rural and urban students, hence the null hypothesis “There is no significant difference in the mean score of cyber safety and security awareness of secondary students with respect to locale of the school”is not accepted and the alternate hypothesis is upheld. Further, from the mean scores, it is evident that those urban students have shown significantly better awareness with a mean score of 195.85.

From the above table, it is also evident that the effect of locale on all the dimension wise mean scores of CSSA was significant at 0.05 level. Hence the second hypothesis “There is no significant difference in the mean score of different dimensions of cyber safety and security awareness of secondary students with respect to the locale of the school” was also not accepted. The mean scores of urban students were found to be higher than that of rural students across all the dimensions.

4.2.3.2.2 Analysis of effect of gender of the student on overall and dimension wise scores of CSSA

To study the effect of gender of the student on the overall CSSA of secondary students, a null hypothesis "There is no significant difference in the mean score of cyber safety and security awareness of secondary students with respect to gender of the student" has been proposed. Further, to analyse the effect of gender of the student on various dimensions of CSSA, another hypothesis "There is no significant difference in the mean score of different dimensions of cyber safety and security awareness of secondary students with respect to gender of the student" was also proposed. ANOVA was performed to analyze the data and the results are given in the following table:

Table 4.45 ANOVA score of effect of Gender on CSSA and its dimensions

		Sum of Squares	df	Mean Square	F	Sig.
Total Awareness Score	**Between Groups**	674624.85	2	337312.42	343.80	.000
	Within Groups	113309733.34	115491	981.11		
	Total	113984358.19	115493			
Psychological Dimension	**Between Groups**	79056.18	2	39528.09	229.71	.000
	Within Groups	19873276.91	115491	172.07		
	Total	19952333.10	115493			
Physical Dimension	**Between Groups**	14388.60	2	7194.30	206.71	.000
	Within Groups	4019478.28	115491	34.80		
	Total	4033866.88	115493			
Legal Dimension	**Between Groups**	14452.68	2	7226.34	265.63	.000
	Within Groups	3141779.47	115491	27.20		
	Total	3156232.16	115493			
Socio-Ethical Dimension	**Between Groups**	47525.96	2	23762.98	449.33	.000

	Within Groups	6107739.32	115491	52.88		
	Total	6155265.29	115493			
Technical Dimension	**Between Groups**	6957.13	2	3478.56	88.24	.000
	Within Groups	4552746.05	115491	39.42		
	Total	4559703.19	115493			

From the above table, it is evident that the obtained F value of 343.80 is significant at 0.01 level. This means that there is a significant difference in the mean score of awareness about cyber safety and security with respect to gender of the students and hence the null hypothesis "There is no significant difference in the mean score of cyber safety and security awareness of secondary students with respect to gender of the student" is not accepted and the alternate hypothesis is upheld.

Similar trend was observed with regard to the effect of gender on the dimension wise scores of CSSA across all the dimensions. Across all dimensions, the F value found to be significant at 0.01 level. Hence the null hypothesis "There is no significant difference in the mean score of different dimensions of cyber safety and security awareness of secondary students with respect to gender of the student" is not accepted.

In order to find out the differences among groups, Duncan post-hoc test has been performed and the results are given in the following table.

Table 4.46 Post hoc analysis of group difference in CSSA with respect to gender of the students

Duncan[a,b] Subset for alpha = 0.05

Gender	N	1	2
Transgender	83	176.30	
Male	53929		189.65
Female	61482		194.42
Sig.		1.000	.090

Means for groups in homogeneous subsets are displayed.

a. Uses Harmonic Mean Sample Size = 248.283.

b. The group sizes are unequal. The harmonic mean of the group sizes is used. Type I error levels are not guaranteed.

The above table shows no significant difference in Total Awareness Scores between Transgender individuals and Males. There is no significant difference in Total Awareness

Scores between Males and Females, although it is borderline significant. These findings suggest that while there are differences in mean Total Awareness Scores between the groups, the only potentially meaningful difference is between Males and Females, where the difference approaches significance.

From the above table it is clear that the mean awareness scores of students vary across the groups. The obtained mean score of female students (194.42) was found to be greater among all the groups and the smallest mean score was observed among transgender students (176.30). Hence it can be concluded that the female students are having higher levels of awareness about cyber safety and security. The mean scores (overall and dimension wise) are plotted in the mean plots below.

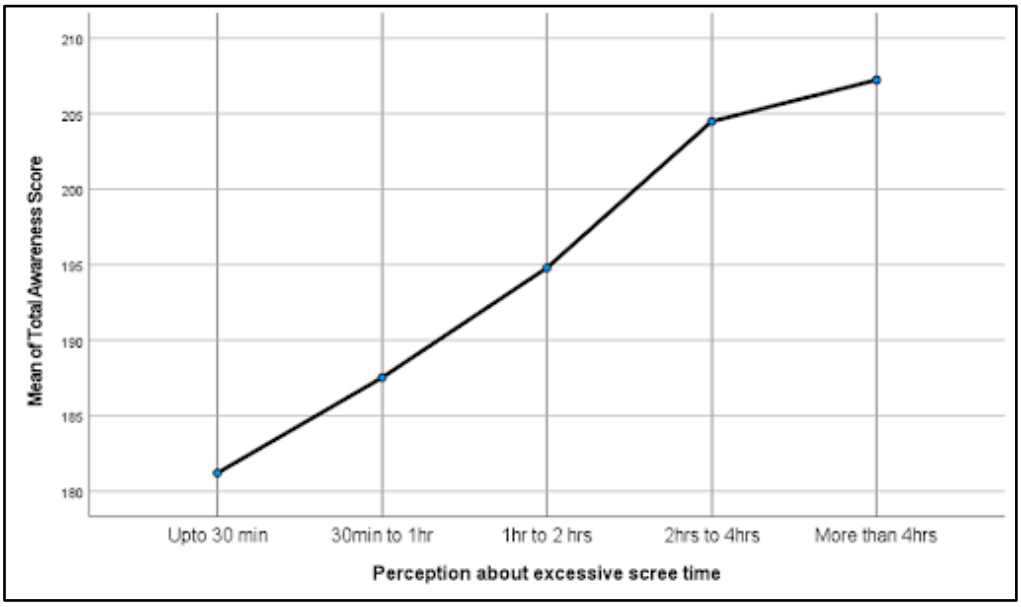


Fig 4.38 Mean plot of group difference in CSSA with respect to gender of the students

Table 4.47 Dimension-wise post hoc analysis of group difference in CSSA with respect to gender of the students (psychological dimension)

Duncan[a,b] Subset for alpha = 0.05

Gender	N	1	2
Transgender	83	31.46	
Male	53929		38.04
Female	61482		39.65
Sig.		1.000	.172

Means for groups in homogeneous subsets are displayed.

a. Uses Harmonic Mean Sample Size = 248.283.

b. The group sizes are unequal. The harmonic mean of the group sizes is used. Type I error levels are not guaranteed.

There is no significant difference in scores for the Psychological Dimension between Transgender and Males. There is no significant difference in scores for the Psychological Dimension between Males and Females at the conventional significance level. These findings suggest that based on the Psychological Dimension, there are no significant differences between Transgender and Males, nor between Males and Females. The differences observed in mean scores across genders do not exceed the critical range for statistical significance as determined by Duncan's test.

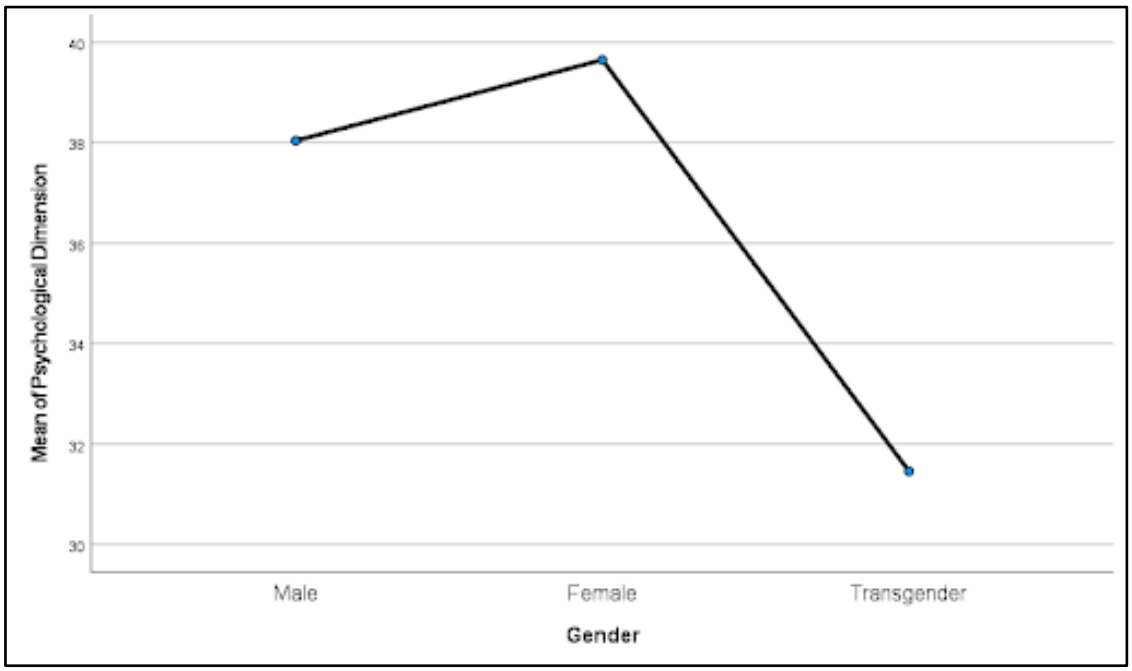


Fig 4.39 Mean plot of group difference in psychological dimension of CSSA with respect to gender of the student.

Table 4.48 Dimension-wise post hoc analysis of group difference in CSSA with respect to gender of the student (physical dimension)

Duncan[a,b] Subset for alpha = 0.05

Gender	N	1	2
Transgender	83	33.25	
Male	53929		35.50
Female	61482		36.19
Sig.		1.000	.190

Means for groups in homogeneous subsets are displayed.

a. Uses Harmonic Mean Sample Size = 248.283.
b. The group sizes are unequal. The harmonic mean of the group sizes is used. Type I error levels are not guaranteed.

There is no significant difference in scores for the Physical Dimension between Transgender and Males. There is no significant difference in scores for the Physical Dimension

between Males and Females at the conventional significance level. These findings suggest that, based on the Physical Dimension, there are no significant differences between Transgender and Males, nor between Males and Females. The observed differences in mean scores across genders do not exceed the critical range for statistical significance as determined by Duncan's test.

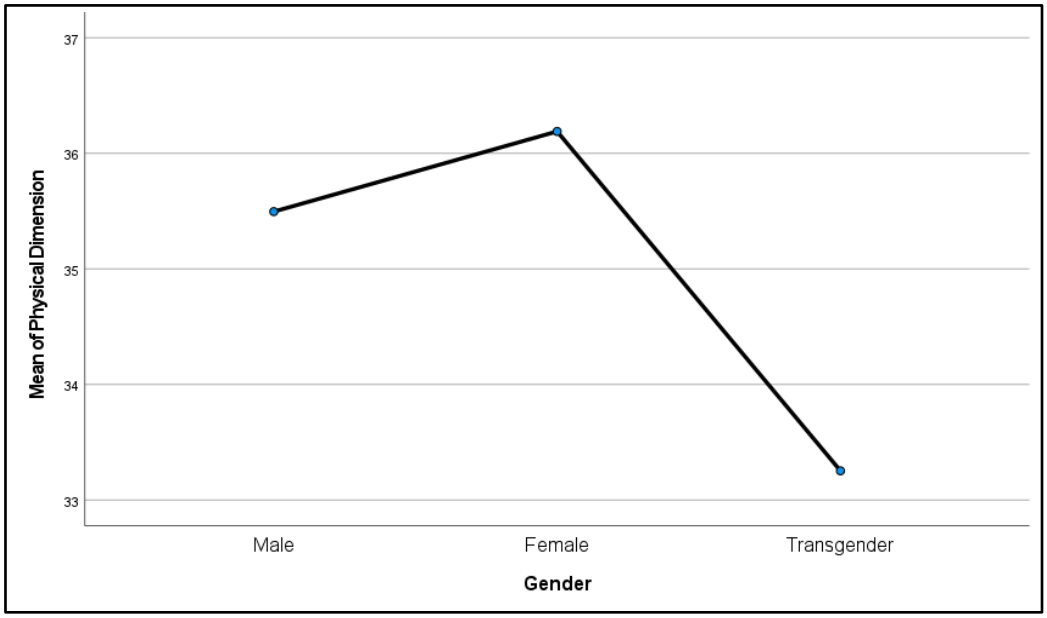


Fig 4.40 Mean plot of group difference in CSSA with respect to gender of the students (Physical Dimension)

Table 4.49 Dimension-wise post-hoc analysis of group difference in CSSA with respect to gender of the students (Legal Dimension)

Duncan[a,b] Subset for alpha = 0.05

Gender	N	1	2
Transgender	83	31.92	
Male	53929		33.19
Female	61482		33.89
Sig.		1.000	.133

Means for groups in homogeneous subsets are displayed.

a. Uses Harmonic Mean Sample Size = 248.283.
b. The group sizes are unequal. The harmonic mean of the group sizes is used. Type I error levels are not guaranteed.

There is no significant difference in scores for the Legal Dimension between Transgender and Males. There is no significant difference in scores for the Legal Dimension between Males and Females at the conventional significance level. These findings suggest that based on the Legal Dimension, there are no significant differences between Transgender and Males, nor between Males and Females. The observed differences in mean scores across

genders do not exceed the critical range for statistical significance as determined by Duncan's test.

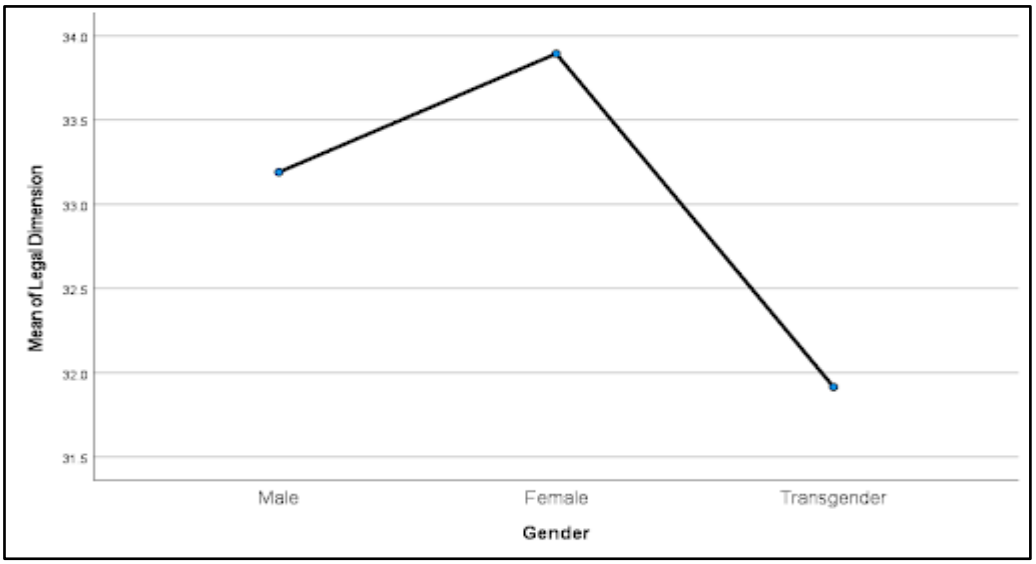


Fig 4.41 Mean plot of group difference in CSSA with respect to gender of the students (Legal dimension)

Table 4.50 Dimension-wisr post-hoc analysis of group difference in CSSA with respect to gender of the students (Socio-Ethical Dimension)

Duncan[a,b] Subset for alpha = 0.05

Gender	N	1	2
Transgender	83	41.19	
Male	53929		42.99
Female	61482		44.27
Sig.		1.000	.050

There is no significant difference in scores for the Socio-Ethical Dimension between Transgender and Males. There is a borderline significant difference in scores for the Socio-Ethical Dimension between Males and Females, suggesting that Females tend to have slightly higher scores compared to Males. These findings suggest that based on the Socio-Ethical Dimension, there are no significant differences between Transgender individuals and Males, but there is a potential difference between Males and Females. The observed difference between Males and Females in mean scores is close to the threshold for statistical significance as determined by Duncan's test.

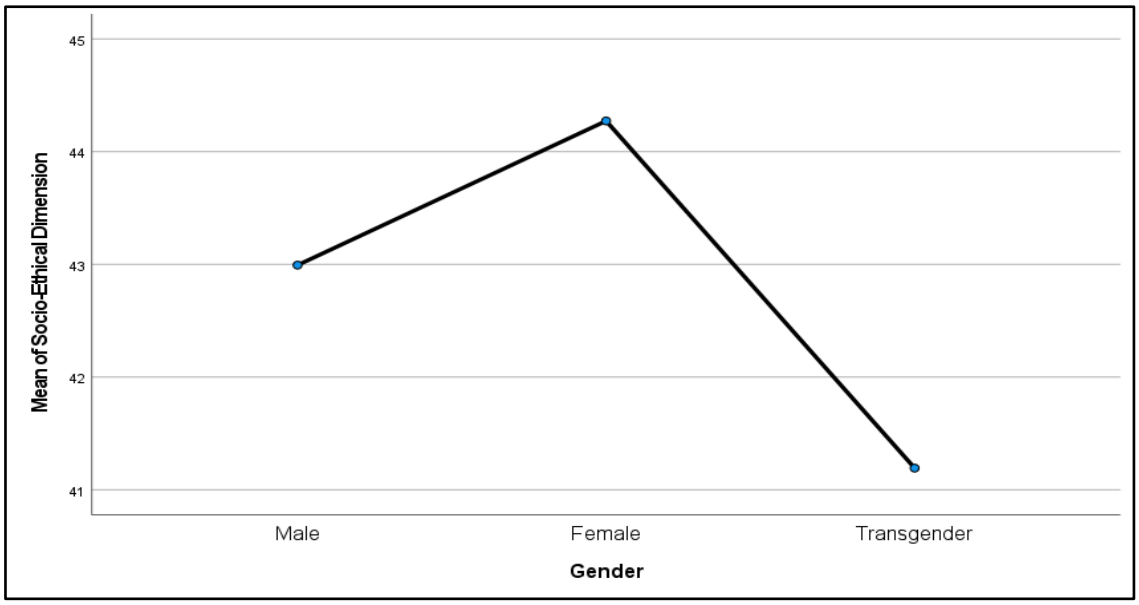


Fig 4.42 Mean plot of group difference in CSSA with respect to gender of the students (Socio-ethical dimension)

Table 4.51 Dimension-wise post-hoc analysis of group difference in CSSA with respect to gender of the students (Technical Dimension)

Duncan[a,b] Subset for alpha = 0.05

Gender	N	1	2
Transgender	83	38.48	
Male	53929		39.93
Female	61482		40.41
Sig.		1.000	.391

Means for groups in homogeneous subsets are displayed.

a. Uses Harmonic Mean Sample Size = 248.283.
b. The group sizes are unequal. The harmonic mean of the group sizes is used. Type I error levels are not guaranteed.

The mean score for the 'Transgender' group is lower compared to both 'Male' and 'Female' groups. However, the significance value (1.000) suggests that this difference is not statistically significant at the 0.05 level.

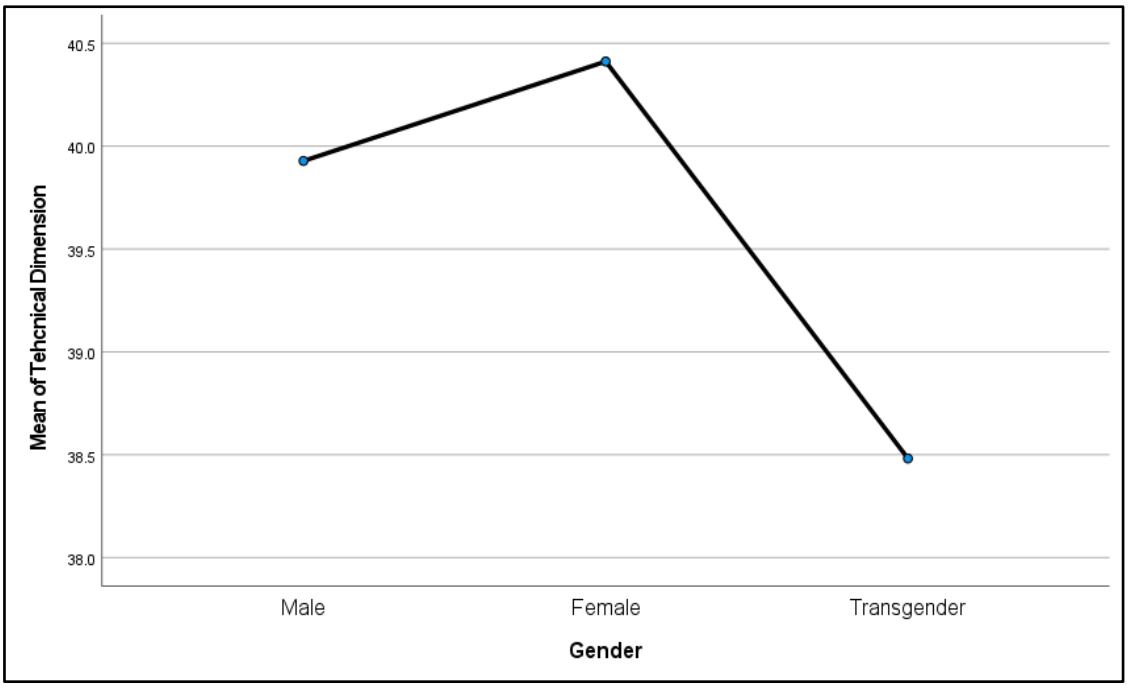


Fig 4.43 Mean plot of group difference in CSSA with respect to gender of the students (Technical dimension)

To study the effect of gender of the student on the overall CSSA of secondary students, a null hypothesis "There is no significant difference in the mean score of cyber safety and security awareness of secondary students with respect to gender of the student" has been proposed. Further, to analyse the effect of gender of the student on various dimensions of CSSA, another hypothesis "There is no significant difference in the mean score of different dimensions of cyber safety and security awareness of secondary students with respect to gender of the student" was also proposed. ANOVA was performed to analyze the data and the results are given in the following table:

4.2.3.2.3 Analysis of effect of standard of the students on overall and dimension wise scores of CSSA

To study the effect of standard of the students on the overall CSSA of secondary students a null hypothesis, there is no significant difference between the mean scores for cyber safety and security awareness among students and their standard with their dimensions has been proposed. further , to analyze the effort of standard of the student on various dimensions of CSSA, another hypothesis "There is no significant difference in the mean score of different dimensions of cyber safety and security awareness of secondary students with respect to standard of the student" was also proposed. ANOVA was performed to analyze the data and the results are given in the following table:

Table 4.52 Dimension-wise ANOVA Score of group difference in CSSA with respect to standards of the students

		Sum of Squares	df	Mean Square	F	Sig.
Total Awareness Score	**Between Groups**	550363.74	3	183454.58	186.72	.000
	Within Groups	113601105.48	115626	982.48		
	Total	114151469.22	115629			
Psychological Dimension	**Between Groups**	107801.60	3	35933.87	208.97	.000
	Within Groups	19882574.14	115626	171.95		
	Total	19990375.75	115629			
Physical Dimension	**Between Groups**	8519.94	3	2839.98	81.46	.000
	Within Groups	4031008.86	115626	34.86		
	Total	4039528.80	115629			
Legal Dimension	**Between Groups**	6164.80	3	2054.93	75.35	.000
	Within Groups	3152999.77	115626	27.26		
	Total	3159164.58	115629			
Socio-Ethical Dimension	**Between Groups**	17914.024	3	5971.34	112.37	.000
	Within Groups	6143881.59	115626	53.13		
	Total	6161795.61	115629			
Technical Dimension	**Between Groups**	13089.489	3	4363.16	110.87	.000
	Within Groups	4550174.13	115626	39.35		
	Total	4563263.62	115629			

The obtained F value is 186.72, which is significant at 0.01 level ($p<0.01$). This means that there exists a significant difference in cyber security and safety awareness with regard to the students studying standard-wise. Hence the null hypothesis stating that there is no significant difference in cyber security awareness among students studying standard has not been accepted and the alternate hypothesis is upheld. In order to find out differences among groups, Duncan's post-hoc test has been performed and the results are given in the below table.

Table 4.53 Dimension-wise post-hoc analysis of group difference in CSSA with respect to standard of the students

Duncan[a,b] Subset for alpha = 0.05

Standard	**N**	**1**	**2**	**3**
9th Standard	38308	189.98		
11th Standard	5450	190.67		
10th Standard	38096		191.70	
12th Standard	33776			195.37
Sig.		.056	1.000	1.000

Means for groups in homogeneous subsets are displayed.

a. Uses Harmonic Mean Sample Size = 15068.936.
b. The group sizes are unequal. The harmonic mean of the group sizes is used. Type I error levels are not guaranteed.

From the above table, it is clear that the mean awareness score of students studying standards across the groups. The obtained mean scores of those students studying 12th standard (195.37) was found to be greater among all the groups and the smallest mean score was observed among students studying 9th standard (189.98). Hence it can be concluded that the students studying in the 12th standard are having a higher level of awareness about cyber safety and security. The mean scores are plotted in the mean plot below.

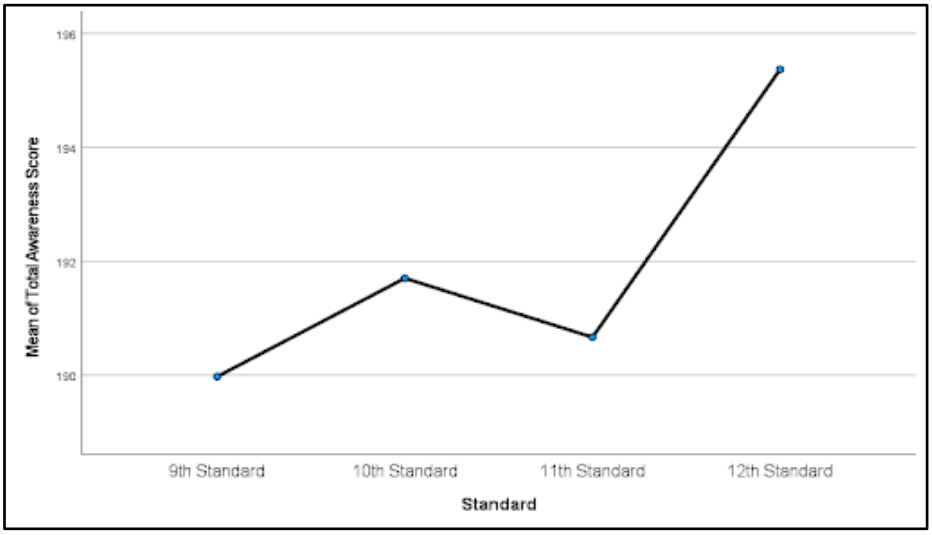


Fig 4.44 Mean plot of group difference in CSSA with respect to standard of the student

Table 4.54 Dimension-wise post-hoc analysis of group difference in CSSA with respect to standard of the students (Psychological Dimension)

Duncan[a,b] Subset for alpha = 0.05

Standard	N	1	2	3	4
9th Standard	38308	37.83			
11th Standard	5450		38.16		
10th Standard	38096			38.85	
12th Standard	33776				40.24
Sig.		1.000	1.000	1.000	1.000

Means for groups in homogeneous subsets are displayed.

a. Uses Harmonic Mean Sample Size = 15068.936.

b. The group sizes are unequal. The harmonic mean of the group sizes is used. Type I error levels are not guaranteed.

With respect to the psychological awareness score, a significant difference was observed between 12th standard and 10th standard with all the other groups. Among all the groups, the mean score of class 12th students were found to have higher than that of other groups. The results are graphically represented below.

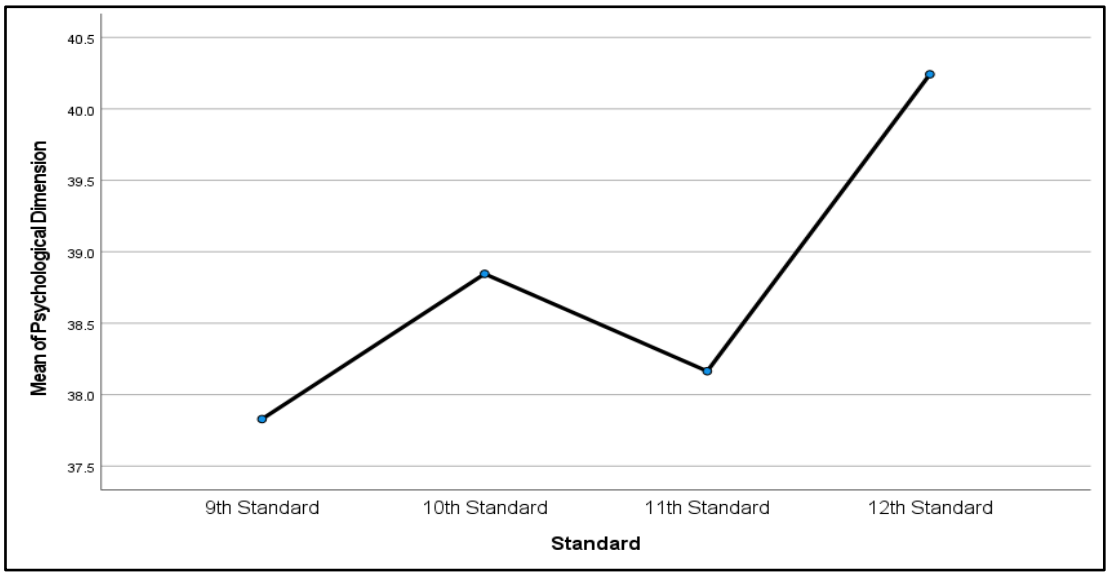


Fig 4.45 Mean plot of group difference in CSSA with respect to standard of the students (Psychological dimension)

Table 4.55 Dimension-wise post-hoc analysis of group difference in CSSA with respect to standard of the students (Physical Dimension)

Duncan[a,b] Subset for alpha = 0.05

Standard	N	1	2	3
9th Standard	38308	35.58		
11th Standard	5450	35.70	35.70	
10th Standard	38096		35.80	
12th Standard	33776			36.26
Sig.		.083	.129	1.000

Means for groups in homogeneous subsets are displayed.

a. Uses Harmonic Mean Sample Size = 15068.936.
b. The group sizes are unequal. The harmonic mean of the group sizes is used. Type I error levels are not guaranteed.

With respect to the physical awareness score, a significant difference was observed between 12th standard and 10th standard with all the other groups. Among all the groups, the mean score of class 12th students were found to have higher than that of other groups. The results are graphically represented below.

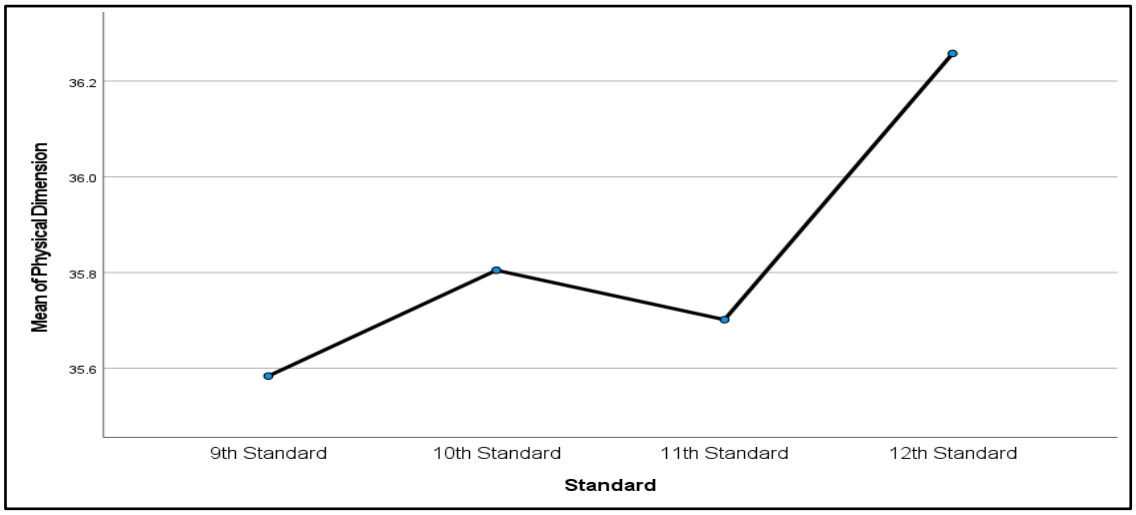


Fig 4.46 Mean plot of group difference in CSSA with respect to standard of the students (Physical Dimension)

Table 4.56 Dimension-wise Post-hoc analysis of group difference in CSSA with respect to standard of the students (Legal Dimension)

Duncan[a,b] Subset for alpha = 0.05

Standard	N	1	2
11th Standard	5450	33.37	
9th Standard	38308	33.38	
10th Standard	38096	33.46	
12th Standard	33776		33.92
Sig.		.180	1.000

Means for groups in homogeneous subsets are displayed.

a. Uses Harmonic Mean Sample Size = 15068.936.

b. The group sizes are unequal. The harmonic mean of the group sizes is used. Type I error levels are not guaranteed.

With respect to the legal dimension of the awareness score, a similar significant difference was observed between the groups. The mean scores of all the groups are closer among each other. The results are graphically represented below.

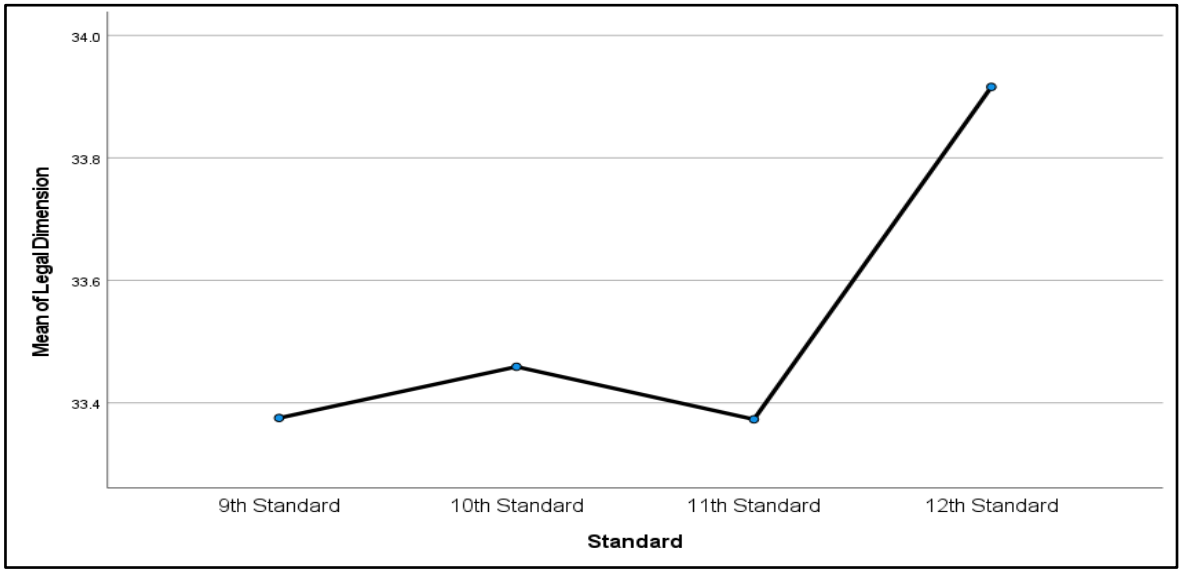


Fig 4.47 Mean plot of group difference in CSSA with respect to standard of the students (legal Dimension)

Table 4.57 Dimension-wise post-hoc analysis of group difference in CSSA with respect to standard of the students (Socio-Ethical Dimension)

Duncan[a,b] Subset for alpha = 0.05

Standard	N	1	2	3
11th Standard	5450	43.32		
9th Standard	38308	43.33		
10th Standard	38096		43.53	
12th Standard	33776			44.27
Sig.		.976	1.000	1.000

Means for groups in homogeneous subsets are displayed.

a. Uses Harmonic Mean Sample Size = 15068.936.

b. The group sizes are unequal. The harmonic mean of the group sizes is used. Type I error levels are not guaranteed.

With respect to the socio-ethical awareness score, a significant difference was observed between the groups. The mean scores of 12th-standard students were found to have higher than that of other groups. The results are graphically represented below.

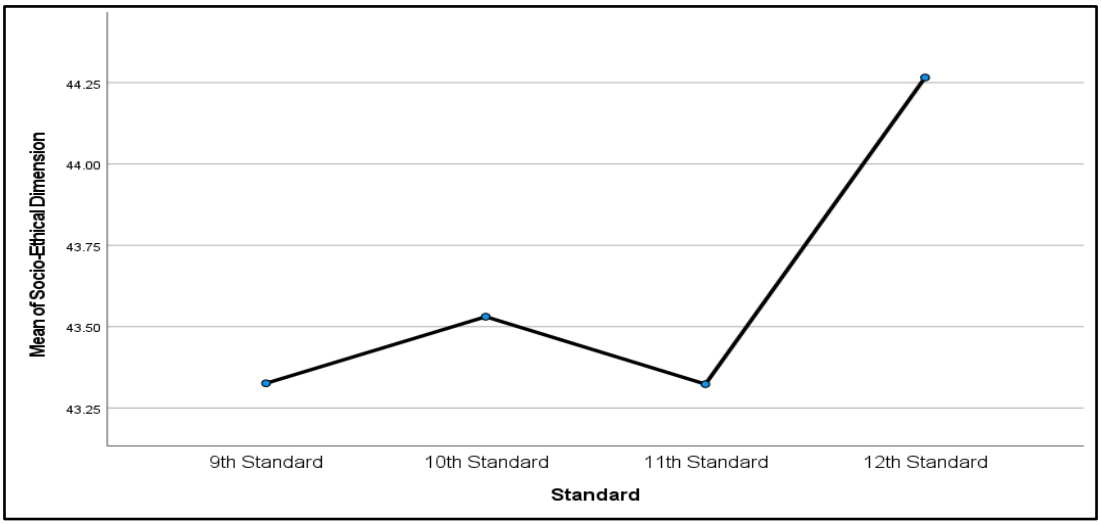


Fig 4.48 Mean plot of group difference in CSSA with respect to standard of the students (Socio Ethical dimension)

Table 4.58 Dimension-wise post-hoc analysis of group difference in CSSA with respect to standard of the students (Technical Dimension)

Duncan[a,b] Subset for alpha = 0.05

Standard	N	1	2	3
9th Standard	38308	39.86		
10th Standard	38096		40.06	
11th Standard	5450		40.11	
12th Standard	33776			40.69
Sig.		1.000	.557	1.000

Means for groups in homogeneous subsets are displayed.

a. Uses Harmonic Mean Sample Size = 15068.936.

b. The group sizes are unequal. The harmonic mean of the group sizes is used. Type I error levels are not guaranteed.

With respect to the technical dimension of the awareness score, a significant difference was observed between the groups. The mean scores of 12th-standard students were found to have higher than that of other groups. The results are graphically represented below.

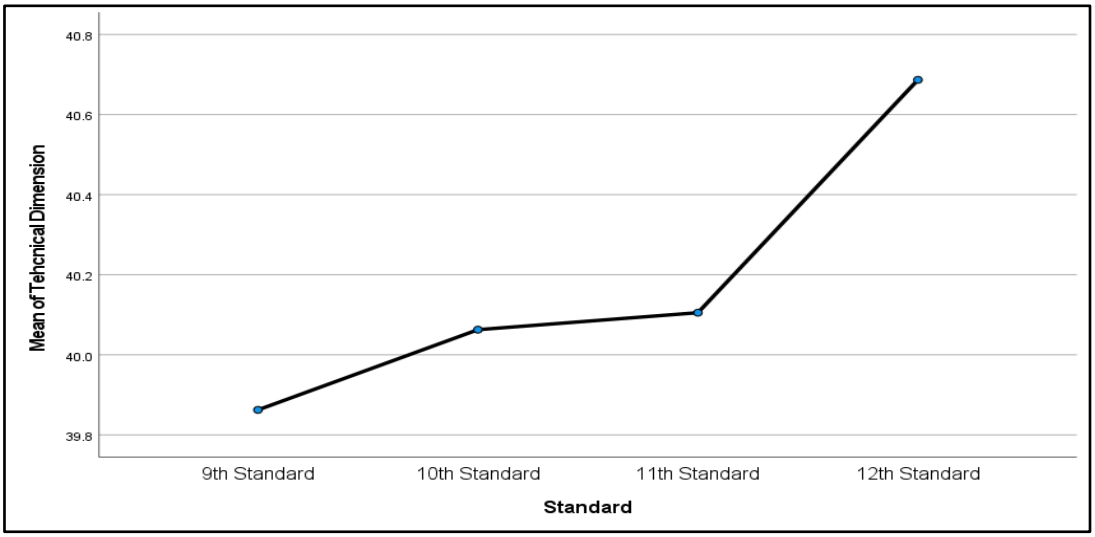


Fig 4.49 Mean plot of group difference in CSSA with respect to standard of the students (Technical dimension)

4.2.3.2.4 Analysis of effect of type of schools of the students on overall and dimension wise scores of CSSA.

To study the effect of the type of schools of the students on the overall CSSA of secondary students a null hypothesis, There is no significant difference between the mean scores for cyber safety and security awareness among students and their type of school with their dimensions has been proposed. further, to analyze the effort of the type of schools of the student on various

dimensions of CSSA, another hypothesis “There is no significant difference in the mean score of different dimensions of cyber safety and security awareness of secondary students with respect to the type of schools of the student” was also proposed. ANOVA was performed to analyze the data and the results are given in the following table:

Table 4.59 Dimension-wise ANOVA Scores of group difference in CSSA with respect to Type of School of the students

		Sum of Squares	df	Mean Square	F	Sig.
Total Awareness Score	**Between Groups**	1141232.25	2	570616.12	583.82	.000
	Within Groups	113010236.97	115627	977.36		
	Total	114151469.22	115629			
Psychological Dimension	**Between Groups**	111614.84	2	55807.42	324.61	.000
	Within Groups	19878760.91	115627	171.92		
	Total	19990375.75	115629			
Physical Dimension	**Between Groups**	29802.69	2	14901.34	429.70	.000
	Within Groups	4009726.10	115627	34.67		
	Total	4039528.80	115629			
Legal Dimension	**Between Groups**	21261.31	2	10630.65	391.72	.000
	Within Groups	3137903.26	115627	27.13		
	Total	3159164.58	115629			
Socio-Ethical Dimension	**Between Groups**	55586.34	2	27793.17	526.29	.000
	Within Groups	6106209.26	115627	52.81		
	Total	6161795.61	115629			
Technical Dimension	**Between Groups**	32518.20	2	16259.10	414.94	.000
	Within Groups	4530745.41	115627	39.18		
	Total	4563263.62	115629			

From the above table, it is evident that the obtained F value of 583.82 is significant at 0.05 level. This means that there is a significant difference in the mean square of awareness about cyber safety and security among type of school, hence the null hypothesis is not accepted and the alternate hypothesis is upheld. Further, from the Sum of Squares, it is evident that those between groups have shown significantly better awareness with a mean square of 337312.42.

Table 4.60 Dimension-wise post-hoc analysis of group difference in CSSA with respect to Type of School of the students

Duncan[a,b] Subset for alpha = 0.05

Type of School	N	1	2	3
Government	97028	190.84		
Aided	6518		195.69	
Private	12084			200.75
Sig.		1.000	1.000	1.000

Means for groups in homogeneous subsets are displayed.

a. Uses Harmonic Mean Sample Size = 12171.291.

b. The group sizes are unequal. The harmonic mean of the group sizes is used. Type I error levels are not guaranteed.

With respect to the overall awareness score, a significant difference was observed between Private and Aided schools with all the other groups. Among all the groups, the mean score of private schools were found to be higher than that of other groups. The results are graphically represented below.

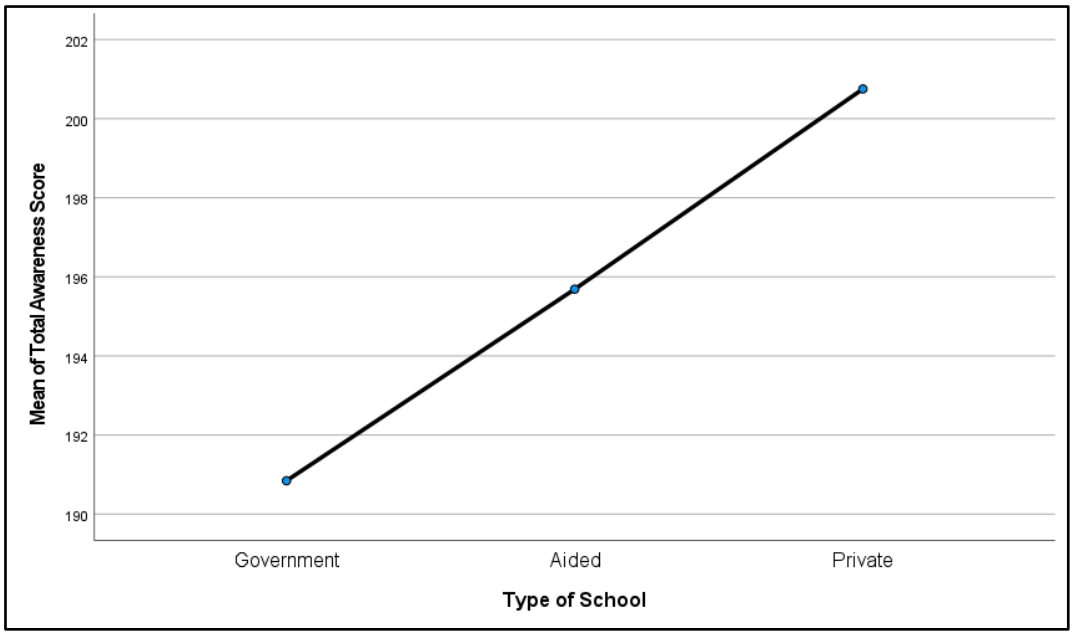


Fig 4.50 Mean plot of group difference in CSSA with respect to Type of School of the students

Table 4.61 Dimension-wise post-hoc analysis of group difference in CSSA with respect to Type of School of the students (Psychological Dimension)

Duncan[a,b] Subset for alpha = 0.05

Type of School	N	1	2	3
Government	97028	38.48		
Aided	6518		39.90	
Private	12084			41.60
Sig.		1.000	1.000	1.000

Means for groups in homogeneous subsets are displayed.

a. Uses Harmonic Mean Sample Size = 12171.291.

b. The group sizes are unequal. The harmonic mean of the group sizes is used. Type I error levels are not guaranteed.

With respect to the psychological awareness score, a significant difference was observed between private and aided schools with all the other groups. Among all the groups, the mean score of private schools were found to be higher than that of other groups. The results are graphically represented below.

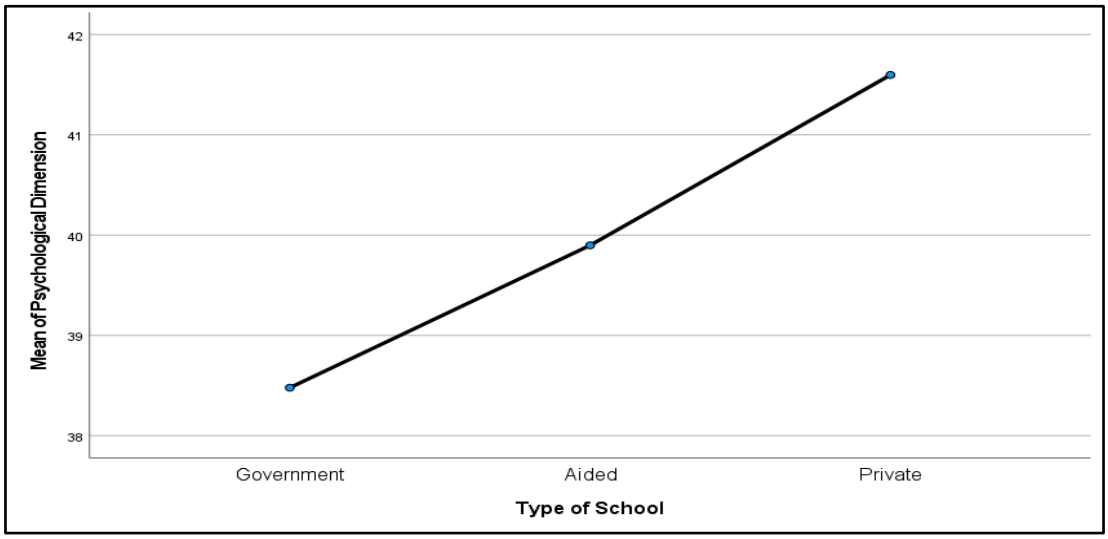


Fig 4.51 Mean plot of group difference in CSSA with respect to Type of School of the student (Psychological dimension)

Table 4.62 Dimension-wise post-hoc analysis of group difference in CSSA with respect to Type of School of the student (Physical Dimension)

Duncan[a,b] Subset for alpha = 0.05

Type of School	N	1	2	3
Government	97028	35.65		
Aided	6518		36.40	
Private	12084			37.26
Sig.		1.000	1.000	1.000

Means for groups in homogeneous subsets are displayed.

a. Uses Harmonic Mean Sample Size = 12171.291.

b. The group sizes are unequal. The harmonic mean of the group sizes is used. Type I error levels are not guaranteed.

With respect to physical awareness score, a similar significant difference was observed between the groups. The mean scores of private schools were found to have slightly higher than that of other groups. The results are graphically represented below.

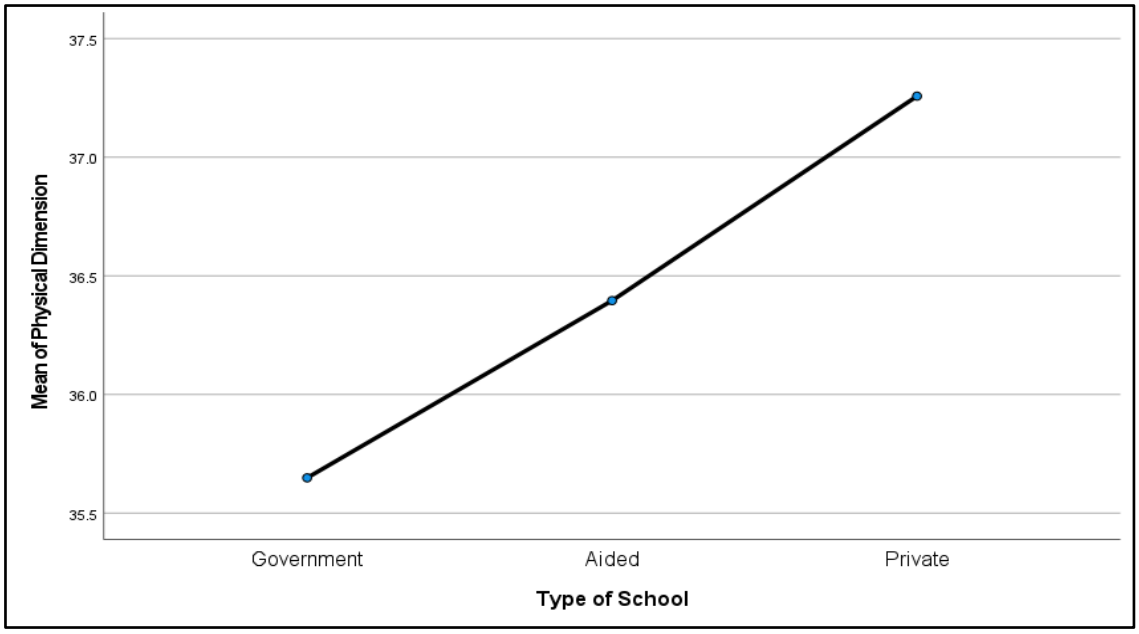


Fig 4.52 Mean plot of group difference in CSSA with respect to Type of School of the student (Physical dimension)

Table 4.63 Dimension-wise post-hoc analysis of group difference in CSSA with respect to Type of School of the student (Legal dimension)

Duncan[a,b] Subset for alpha = 0.05

Type of School	N	1	2	3
Government	97028	33.38		
Aided	6518		34.03	
Private	12084			34.74
Sig.		1.000	1.000	1.000

Means for groups in homogeneous subsets are displayed.

a. Uses Harmonic Mean Sample Size = 12171.291.

b. The group sizes are unequal. The harmonic mean of the group sizes is used. Type I error levels are not guaranteed.

With respect to the legal dimension of the awareness score, a similar significant difference was observed between the groups. The mean scores of all the groups are closer among each other. The results are graphically represented below.

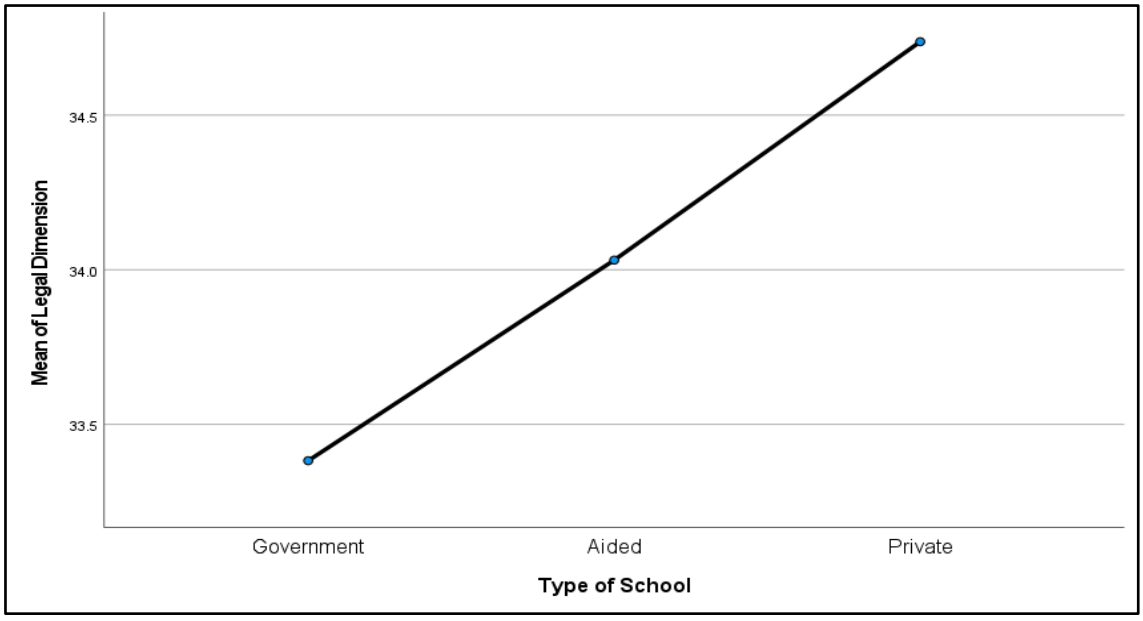


Fig 4.53 Mean plot of group difference in CSSA with respect to Type of School of the student (Legal dimension)

Table 4.64 Dimension-wise post-hoc analysis of group difference in CSSA with respect to Type of School of the student (Socio-Ethical Dimension)

Duncan[a,b] Subset for alpha = 0.05

Type of School	N	1	2	3
Government	97028	43.38		
Aided	6518		44.49	
Private	12084			45.55
Sig.		1.000	1.000	1.000

Means for groups in homogeneous subsets are displayed.

a. Uses Harmonic Mean Sample Size = 12171.291.

b. The group sizes are unequal. The harmonic mean of the group sizes is used. Type I error levels are not guaranteed.

With respect to the socio-ethical awareness score, a significant difference was observed between the groups. The mean scores of private schools were found to have higher than that of other groups. The results are graphically represented below.

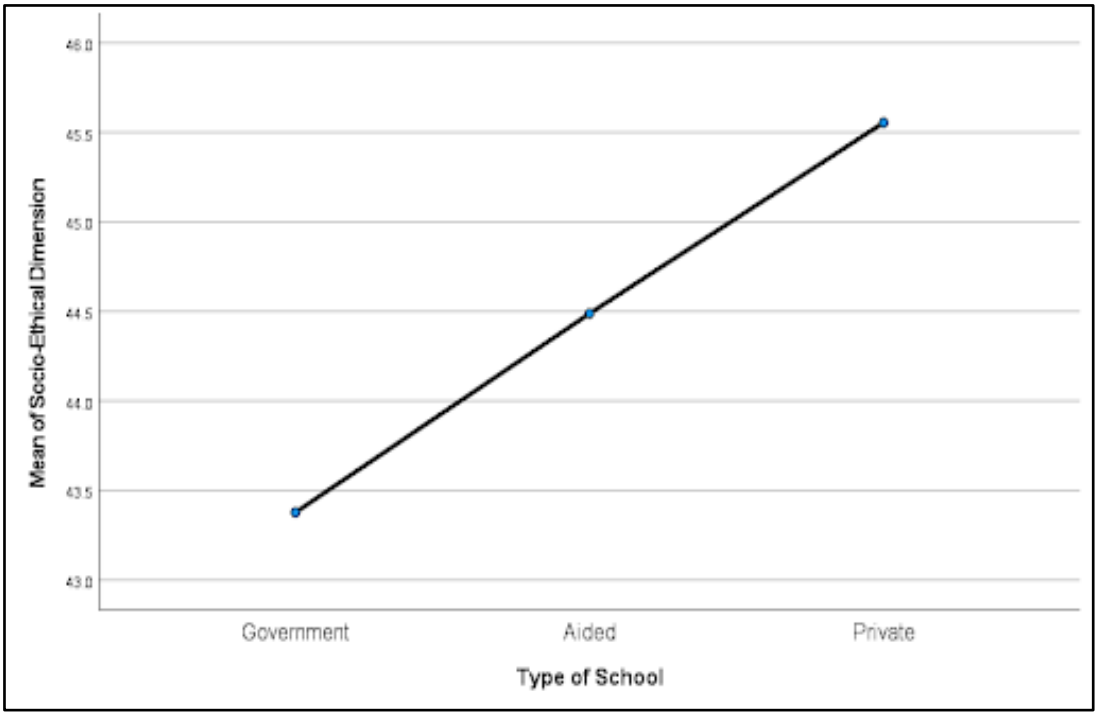


Fig 4.54 Mean plot of group difference in CSSA with respect to Type of School (Socio-ethical dimension)

Table 4.65 Dimension-wise post-hoc analysis of group difference in CSSA with respect to Type of School of the student (Technical Dimension)

Duncan[a,b] Subset for alpha = 0.05

Type of School	N	1	2	3
Government	97028	39.96		
Aided	6518		40.87	
Private	12084			41.61
Sig.		1.000	1.000	1.000

Means for groups in homogeneous subsets are displayed.

a. Uses Harmonic Mean Sample Size = 12171.291.

b. The group sizes are unequal. The harmonic mean of the group sizes is used. Type I error levels are not guaranteed.

With respect to the technical dimension of the awareness score, a significant difference was observed between the groups. The mean scores of private schools were found to be higher than that of other groups. The results are graphically represented below.

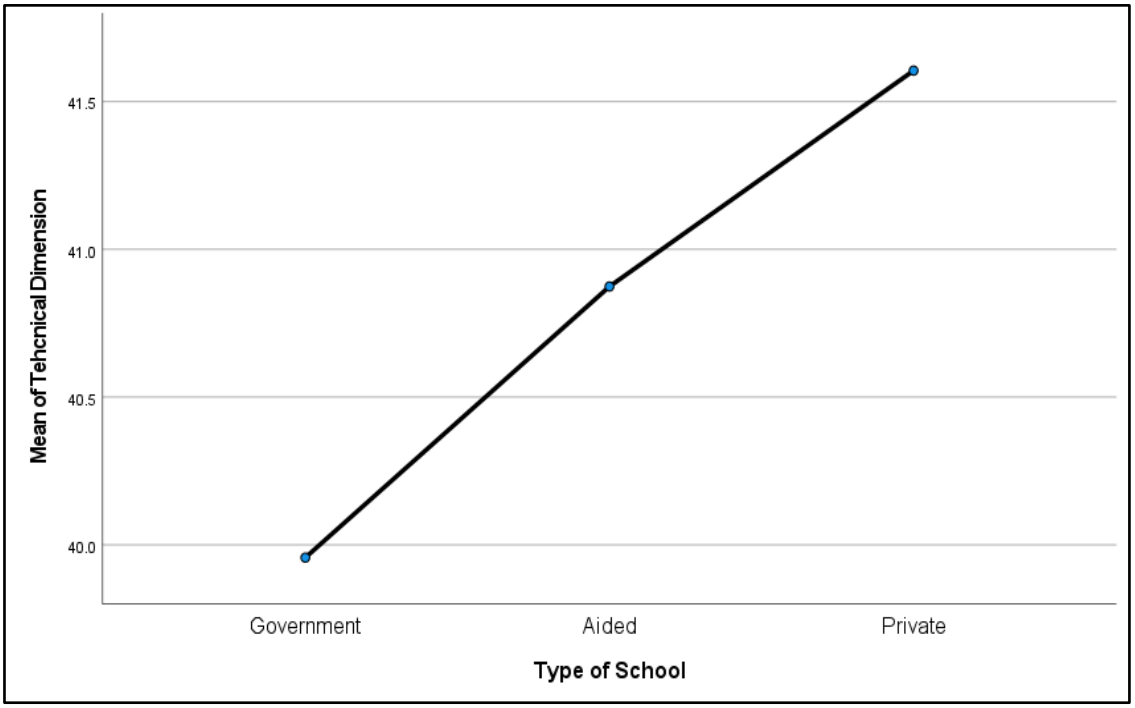


Fig 4.55 Mean plot of group difference in CSSA with respect to Type of School (Technical Dimension)

CHAPTER 5: SUMMARY AND CONCLUSION

5.1. Genesis of the Problem

In order to give secondary students the necessary abilities for successfully navigating the digital world, the Government has taken steps to increase awareness of cyber safety and security. These programs seek to teach children about internet safety, how to use the internet responsibly, and how to secure their personal data. Through the inclusion of cyber safety in the curriculum, the government guarantees that students acquire the resilience and knowledge needed to protect themselves in the digital world.

5.2. Need and Significance of the Study

In today's digital world, the study on cyber safety and security awareness among secondary students has become extremely important. As technology advances, adolescents become more entrenched in the online world, leaving them vulnerable to a variety of cyber risks. Understanding the level of awareness about cyber safety and security is critical for several reasons. Adolescents constitute a sizable proportion of internet users, and they are frequently involved in online activities such as social networking, gaming, and academic research. Numerous individuals may be unaware of the hazards involved with these activities, such as cyberbullying, identity theft, phishing, and exposure to unsuitable information. Educators, legislators, and parents may identify knowledge gaps and build tailored educational programs to provide children with the skills they need to securely navigate the online world by analyzing their awareness levels.

Fostering a culture of cyber safety and security among secondary students is critical for the overall well-being of society. As digital natives, these adolescents are both consumers and possible contributors to the digital ecosystem. The education system of the country may encourage responsible digital citizenship and reduce the possible negative repercussions of cyber events by teaching children the necessity of adopting safe online behaviors and understanding the ramifications of their digital footprint.

The findings of this research can help to shape school curricula and educational initiatives that are tailored to secondary students' specific needs. Integrating cyber safety and security education into the school curriculum may provide students with the information and skills necessary for safeguarding themselves online, resulting in a safer digital world for everyone.

Furthermore, identifying the elements that influence students' awareness of cyber safety and security can facilitate targeted interventions. Factors such as socioeconomic status, access to technology, parental supervision, and peer influence could affect student's views and actions about online safety. Identifying these elements enables stakeholders to successfully implement prevention techniques and encourage healthy online habits.

The study on secondary students' awareness of cyber safety and security is critical for ensuring the behavior of adolescents' well-being in the digital era. By measuring students'

knowledge, analyzing the driving elements, and implementing tailored interventions, we can help them navigate the online world securely and responsibly, eventually contributing to a more secure digital future for everyone.

5.3. Statement of the Problem

In today's digital era, the behavior of adolescents' extensive utilization of the internet and digital gadgets has created serious concerns about cyber safety and security. Secondary students, particularly those in grades IX-XII, are increasingly involved in online activities for education, social connection, and amusement. While the internet has many advantages, it also exposes students to a variety of challenges, including cyberbullying, identity theft, online predators, and inappropriate information. Despite these hazards, there needs to be more complete information on secondary students' levels of awareness and ability to face these challenges safely.

This study aims to assess the level of knowledge and comprehension of cyber safety and security concerns among secondary students. It intends to identify knowledge gaps and evaluate the performance of current educational programs that address these challenges. The study will provide insight into students' behaviors and perceptions about online safety. For this purpose, the project aims to develop a cyber safety and security awareness scale, assess students' awareness levels, analyze and identify dimensions, and create an intervention package. Hence the problem statement is framed as **"*A Study of the Awareness on Cyber safety and Security Among Secondary Students (Class IX to XII)*".**

5.4. Operational Definitions

The terms used in this study are operationally defined as follows.

5.4.1 Awareness

Awareness is the quality or state of being aware : knowledge and understanding that something is happening or exists (Merriam-webster, 2024). In this study an awareness for teachers is referred to as an organized educational programme designed to give instructors the knowledge, skills, and practices they need to comprehend and apply cyber safety and security measures in learning environments.

5.4.2 Cyber Safety and Security

According to Merriam-Webster, cyber safety is the safe practices when using the Internet to prevent personal attacks or criminal activity. Cybersecurity is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks (Kaspersky, 2024). In this study Cyber Safety and Security refer to teachers who understand how to keep themselves and their students safe online and are practicing cyber safety and security. It involves educating students on how to be responsible online, accessing the internet safely, creating strong passwords, and identifying and addressing online threats including scams and cyberbullying.

5.4.3 Secondary School Students in India

Secondary school students are defined as individuals who are enrolled in grades IX through XII within the Indian educational system. These students typically range in age from approximately 14 to 18 years.

5.5. Variables of the Study

Variables are the factors involved in addressing the research problem, which leads to the closure of the research gap. These attributes ought to impact one another. The current study investigates secondary students' levels of awareness of cyber safety and security. Hence, the following independent and dependent variables were identified for the investigation of the study:

- **Independent Variable**

  An independent variable is a variable that has been manipulated. The independent variable is purposely manipulated during observation to determine its relationship with the dependent variable. So the demographic factors Gender, Standard, States/UTs, Type of School, Locality of the school and Medium of Instruction are considered as independent variables.

- **Dependent Variable**

  The dependent variable is the level of awareness of cyber safety and security among secondary-stage students. This variable represents the degree to which students understand and are informed about various aspects of cyber safety and security, such as recognizing cyber threats, understanding safe online practices, and knowing how to protect personal information online. This awareness can be measured through surveys, questionnaires, or assessments designed to evaluate students' knowledge and attitudes towards cyber safety and security issues.

5.6. Research Question

1. What is the awareness level of secondary students on cyber safety and security?
2. What are the dimensions in which secondary students lack awareness of cyber safety and security?

5.7. Objectives of the Study

1. To evaluate the level of awareness and understanding of cyber safety and security among secondary-stage students.
2. To study the difference in awareness on cyber safety and security among secondary school students with respect to various subgroups.
3. To study the difference in different dimensions of cyber safety and security awareness among secondary school students with respect to various subgroups.

5.8. Hypotheses of the Study

To undertake a meaningful analysis, the following hypotheses were proposed. There are 16 hypotheses which were clubbed under three broad hypotheses as given below:

H_1: There is no significant difference in the mean score of cyber safety and security awareness of secondary students with respect to their/ the

1. Access to Internet at home
2. Possession of personal email ID
3. Participation in ICT courses
4. Availability of digital devices at home
5. Availability of own digital devices
6. Possession of personal social media account
7. Duration of use of devices per day
8. Perception about excessive screen time

H_2: There is no significant difference in the mean score of cyber safety and security awareness of secondary students with respect to

1. Locale of the school
2. Gender of the student
3. Standard in which the students are studying
4. Type of school

H_3: There is no significant difference in the mean score of different dimensions of cyber safety and security awareness of secondary students with respect to

1. Locale of the school
2. Gender of the student
3. Standard in which the students are studying
4. Type of school

5.9. Design of the Study

The study used a survey method, a quantitative research technique that optimizes descriptive and inferential statistics, to look into students' awareness of cyber safety and security at the national level.

Survey research is a popular approach in the social sciences because it allows researchers to collect data on various topics related to people's or groups' behavior, ideas, and feelings. The goals of survey research are to describe a population, identify group characteristics, describe features and characteristics of study interest, explain a phenomenon, or explain how variables are connected (Buchanan & Hvizdak, 2009). Online surveys are widely utilized in educational research (Roberts & Allen, 2015). Online surveys are growing more popular. Online surveys are becoming increasingly popular, maybe because they are a simple, convenient, and cost-effective way to collect data (Andrade, 2020). In recent decades, the two most popular social science methods for gathering large-scale recreation data were an online survey and a random digit dial telephone survey. Both strategies have demonstrated efficacy in providing a respectable response rate at a reasonable cost (Loomis & Paterson, 2018).

Online surveys are useful but require a high response rate, which is a key factor for assessing survey quality (Wu et al., 2022). Self-administered surveys have gradually supplanted in-person and telephone surveys, as seen by a historical overview of data-gathering technologies. The usage of online surveys has increased significantly in recent years due to technological advancements (de Rada, 2022). Compared to traditional surveys, administering online surveys is quicker and less costly (Castorena et al., 2023).

5.10. Sample

5.10.1 Population of the Study

The population of the study refers to all the secondary school students (from IX Standard to XII standard) studying in any school, whether Government, Private or Aided school, from all 28 - States and 8 Union Territories in India. There are 6.7 crore students enrolled in secondary education in the 2021-22 session (MoE, 2021). Furthermore, every student who uses the internet in accordance with the eligibility conditions.

5.10.2 Sampling Technique

The process of choosing a small group from a vast population to serve as the actual representation of that population is known as sampling. In the context of a large and geographically dispersed population, a more complex technique known as multistage sampling is employed. Multistage sampling is a complex form of cluster sampling in which the selection of samples is carried out in multiple stages (Cochran, 1977). At each stage, the population is divided into clusters or groups, and a random sample of these clusters is selected. Within each selected cluster, further sampling is done to select smaller units, and this process is repeated as necessary.

Given the vast geographical size and diversity of the population, the documented report utilized a four-phase sampling process to create the final sample for the investigation. In the first phase, the sample encompassed the entire population across all 28 states and 8 Union Territories (UTs). In the second phase, the sample included the entire population across all school boards. The third phase focused on categorizing data by school type, covering private, government, and aided schools, and including their entire student populations. In the fourth phase, the sample included all students from grades IX to XII across the schools. Only students who were using the Internet were included in the final sample for this study.

The sample was collected in four phases:

Phase 1: Selection of States and Union Territories.

The first phase involved choosing every single person living in all 28 states and 8 Union Territories (UTs) in India, all 36 entities were taken. Ensuring geographic coverage and variety, this phase captured the whole range of regional variances and traits.

Phase 2: Selection of School Boards.

In the second phase, every student in every state and UT across all approved school boards was included in the sample. This stage was essential to creating a thorough depiction of the educational environment by incorporating the various curricula and educational systems.

Phase 3: Selection of School Type.

The third phase involved selecting the entire population of students from all demographic groups attending various school kinds, such as government, private, and aided. This classification made sure that varied school settings were included, which reflected the various financial and administrative systems found in the educational system.

Phase 4: Selection of Student Selection.

In the fourth phase, all students across all the schools in grades IX through XII were included in the sample wherein purposive sampling was used as only the students using the Internet were included as the sample of this study.

5.10.3 Sample Size

The sample coverage was 1,15,632 secondary school students (from IX Standard to XII) studying in any school, whether Government, Private, or Aided school, from all 28 Indian States and 8 Union Territories.

5.11. Instruments used in the Study

An awareness instrument with five aspects of cyber safety and security was developed, and validated, and reliability was achieved through pilot testing.

It was determined to employ an online survey for data collection because of the unique nature of the study, as rating scales are thought to be an effective technique for gathering data in descriptive research (Lobe, Simoes, & Zaman 2009). When collecting information from a large sample, a rating scale is a more practical and effective method (Coolican, 2004; Quinn, 2013).

Due to the unique nature of this research project, it was hard to find the appropriate rating scale; a rating scale was created in order to gather relevant information from the population.

The study used an online survey method with a quantitative design; therefore, creating a tool to collect the required data was unavoidable. The research team examined a wide range of relevant literature in order to construct the tool "Cyber Safety and Security Awareness Scale (CSSAS) for Secondary Students," including country reports, peer-reviewed research articles from India and abroad, cyber safety and security guidelines for students from various national and international agencies, policy documents from India and abroad, expert opinions, etc. Dimensions were determined, and the five-point awareness was developed. The scale has five dimensions: Psychological, Physical, Legal, Socio-ethical, and Technical. Each dimension has items categorized as Strongly Agree, Agree, Undecided, Disagree and Strongly Disagree.

5.11.1 Description of the Tool

A five-point rating scale/ awareness tool with five dimensions on cyber safety and security was constructed, validated, and reliability was achieved by going through pilot testing. A Google form was created in English language and translated into Hindi also for the collection of data and the link was shared with all the 36 states and UTs of India for the purpose of collecting

data from secondary school students for the study. Five dimensions of the rating scale are shown below:

Fig 5.1: Dimension coverage

The awareness scale consists of 5 dimensions with 58 items with the 5 responses, namely; strongly agree/agree/ undecided/ disagree/ strongly disagree. Each dimension consists of items with true or false connotations with respect to cyber safety and security. The following table presents dimension-wise items with true/ false connotations.

Table 5.1: Items coverage- Dimension wise

Dimension	True	False	Total
Psychological	12	0	12
Physical	8	3	11
Legal	5	5	10
Socio-ethical	6	7	13
Technical	6	6	12
Total	**37**	**21**	**58**

5.11.2 Pilot Study

A feasibility study, sometimes called a pilot study, is a small-scale investigation carried out before a more extensive, full-scale investigation. It serves as a trial run to evaluate the viability, usefulness, and efficacy of the techniques and protocols intended for the primary study. A pilot study was done on a small sample of secondary students. A sample of 302 secondary students was chosen, and the research tool was administered to them to establish the reliability, viability, usefulness, and efficacy of the research tool.

5.11.3 Validity and Reliability

Validation of Tool: The validity and reliability of the scales employed in research are critical aspects that allow the research to provide useful results. For this reason, it is important to understand how researchers appropriately assess the scales' reliability and validity (Surucu & Maslakci, 2020). A research study may comprise only part of the methodological subspace's elements, which include scientific standards, procedures, and principles. Examples of these elements are validity systems. This subspace is utilized in substantive research to establish knowledge claims and comprises information derived from methodological research (Lund, 2022).

The literature synthesis produced themes and codes for item development in scale based on worldwide and Indian research papers, reports, and policy guidelines, as well as the identified research deficit. The expert members structured the questions and items on the background variables and dimensions of the scale using the themes and codes. The scale contains five dimensions: psychological, physical, legal, socio-ethical, and technical. Individual Items were developed using the dimensions. The items were labeled as Strongly Agree, Agree, Undecided, Disagree and Strongly Disagree. The scale has three parts, excluding the need and objective of the study, the Consent Section;

Part 1: Nature of distribution of samples across sub-groups.

Part 2: Analysis of data with regard to ICT/Digital Exposure

Part 3: Analysis of data with regard to awareness about cyber safety and security

The developed questions on the background variables and items under each dimension were then examined for face validity and content validity by the national-level experts. Based on their validity examination, some items were removed, and a few were added.

- **Face Validity:** Face validity was checked by the research team members first, and then by the Program Coordinator, 80 questions and 5 dimensions were finalized.
- **Content Validity**. The rating scale was validated by 7 experts in the field. Later, the panel of experts was formed based on expertise in psychology, sociology, law, and educational technology; a minimum of five years of experience in concerned fields was required. Three professors and four assistant professors constituted the panel of experts.

The experts' suggestions regarding objectivity, and suitability of items were taken into consideration. Language difficulty was removed by replacing difficult words with easy ones. In the final rating scale out of 80 items, 62 items were selected and reframed according to the need of the study and the rest were removed. All the suggestions given by experts were

incorporated into the final tool. It is only after the validation; that the tool was administered to the sample.

To determine the flaws and limitations and to achieve reliability and validity of the rating scale, pilot testing was done on a small sample of 302 secondary school students. It enables us to refine the instrument and make necessary improvements before the final implementation. A pilot test was conducted on 130 students to ensure the accuracy of items and whether it addressed research questions or not.

Reliability of Research Tool:

Reliability refers to the consistency and stability of a measurement over repeated administrations or observations. A reliability score close to 1.0 indicates a high level of consistency, meaning that the measurement is highly dependable and yields similar results under consistent conditions. The statistical analysis was conducted using version 28.0 of the Statistical Package for the Social Sciences (SPSS). Cronbach's alpha was used to determine the CSSAS quality score's internal consistency. A reliability score of 0.9933 was derived from statistical analyses, indicating that the measurement instrument has demonstrated exceptional reliability in the context of the research study. In research, a reliability score of 0.9933 typically indicates a very high level of reliability of the tool. It also suggests that the measurement instrument or tool used in the study demonstrates an extremely high level of consistency and stability. This high reliability score implies that the measurement is highly trustworthy and can be relied upon to produce consistent and accurate results across multiple administrations or observations.

5.12 Limitations and Constraints

This nationwide quantitative study has its own limitations. They are limited to Age range, educational setting, Coverage of dimensions, Research method, School education, and coverage of languages in tools.

- **Age Range:** The study focused solely on students in grades 9–12, omitting younger or older age groups. This delimitation ensures a specific assessment of cyber safety and security awareness within the context of secondary school.
- **Educational Setting:** Students enrolled in government, private, and aided schools were the only subjects of the study; homeschoolers and participants in alternative education programs were not included. An investigation in a more homogeneous sample and context was made possible by this delimitation.
- **Dimensions of Cyber Safety and Security:** The study concentrated only on five dimensions of cyber safety and security that are pertinent to students in grades 9 through 12, including Psychological, Physical, Legal, Socio-ethical and Technical. This boundary guarantees a targeted analysis of the most important cyber safety and security concerns that affect the intended sample.
- **Research Method:** The study adopted online surveys through Google Forms and quantitative analysis.
- **School Education:** The study focused on students from school education only, higher education was not included in the study.

- **Language coverage:** The tool of the study was prepared in English and Hindi.

5.13. Major Findings of the Study

Nature of distribution of sample across subgroups

State-wise distribution of sample with regard to Gender

The Findings showed that females are the most populous gender group in 21 states and UTs, with Delhi having the highest proportion at 56.8%. In contrast, males are the majority in 15 states and UTs, with Uttar Pradesh exhibiting a significant male majority at 54%, while transgender individuals in Chandigarh represent a minority at 0.5%.

State-wise distribution of sample with regard to Standard

The finding showed that the state-wise data reveals significant variation in student enrollments by standard, with Delhi and Punjab having notably high enrollments in the 10th and 11th standards, while Mizoram leads in the 12th standard with 31.7% of its student population. Delhi also has the highest enrollment in the 9th standard, accounting for 34.5% of its total student population, indicating a strong focus on secondary education.

State-wise distribution of sample with regard to Type of School

Findings showed that Government schools are most common in states like Uttar Pradesh, Madhya Pradesh, and Odisha. Aided schools are prominent in Goa and Delhi, while private schools are notably present in Nagaland, Punjab, and Delhi.

State-wise distribution of sample with regard to the Locality of the school

The finding showed that Punjab has the highest percentage of rural schools at 67.5%, highlighting a strong focus on rural education. In contrast, Delhi has the highest percentage of urban schools at 82.4%, followed by Chandigarh at 81.5%, indicating a concentration of schools in urban areas.

Analysis of data with regard to ICT/Digital Exposure

Gender-wise Distribution of the Internet access at home

The Finding showed that Males have the highest percentage of Internet access at home at 88.6%, while transgender individuals have the lowest at 80.8%.

Gender-wise Distribution of the Email ID

From the above table 4.6, shows that Males have the highest percentage of individuals with an Email ID (80.5%), followed by transgender individuals (74.0%), and females (69.6%). In terms of not having an Email ID, females have the highest percentage (30.4%), followed by transgender individuals (26.0%), and males (19.5%).

Gender-wise Distribution of use of Digital Devices per day

The findings showed that Females slightly favor 30 minutes to 1 hour usage (28.8%) and males slightly higher in the 1 to 2 hours category (27.7%), while transgender individuals predominantly use devices for less than 30 minutes daily (35.6%).

Gender-wise Distribution of Perception about Excessive Screen Time

The Findings showed that Females perceive spending up to 30 minutes on screens the most (32.0%), while transgender individuals show a notable preference for shorter screen times (43.4%), contrasting with males who perceive 25.5% spending up to 30 minutes and 21.1% spending 1 to 2 hours on screens.

Gender-wise Distribution of participation in courses related to ICT

From Table 4.9, transgender individuals exhibit the highest percentage of participation in ICT courses, with 65.3% engaging in such courses. This finding suggests that transgender individuals show a strong interest and involvement in ICT education compared to females and males, based on the available data.

Standard wise Distribution of Internet access at home

From Table 4.10, the 12th standard students have the highest percentage of internet access at 88.9%. Following closely behind are students in the 10th standard, with 88.4% having internet access, showing a similar strong adoption of digital connectivity. In the 11th standard, 88.3% of students have internet access. Among the 9th standard students, 87.2% have internet access, reflecting a slightly lower but still significant level of connectivity compared to higher standards.

Standard-wise Distribution of the Email ID

In Table 4.11, the 12th standard students have the highest percentage of email ID ownership at 82.7%. Following closely behind are students in the 11th standard, with 76.9% having email IDs, showing a substantial engagement with digital platforms for communication. In the 10th standard, 73.6% of students possess email IDs, reflecting a significant presence but slightly lower than the upper secondary levels. Among the 9th standard students, 68.5% have email IDs, demonstrating a growing but relatively lower uptake compared to higher standards.

Standard-wise Distribution of Use of Digital Devices per day

From Table 4.12, 10th Standard has the highest percentage of students spending 1 hour to 2 hours on digital devices per day is 26.6%. 11th Standard has 24.6% of students spending 1 hour to 2 hours on digital devices daily, which is the highest among the given categories. 12th Standard has the highest percentage here also for 1 hour to 2 hours, at 29.1%. 9th Standard has the highest percentage for 1 hour to 2 hours, with 24.6%.

Standard-wise Distribution of Excessive screen time

From Table 4.13, the result reveals that different standards exhibit varied screen time habits, with the 9th standard showing the highest percentage (25.5%) of students spending 30 minutes to 1 hour on screens, while the 12th standard has the highest proportion (19.2%) spending more than 4 hours daily.

Standard-wise Distribution of participation in courses related to ICT

From Table 4.14, The findings indicate that ICT course participation is highest among students in the 11th standard (53.3%), followed closely by the 10th standard (50.8%), revealing varying

levels of engagement across different grades and highlighting potential curricular differences and student interest.

Type of School-wise Distribution of Internet Access at Home

From Table 4.15, The finding shows that internet access at home is highest among students in private schools (91.9%), followed closely by aided (88.5%) and government schools (87.6%), highlighting widespread access across school types and emphasizing its crucial role in supporting online learning and educational connectivity.

Type of School-wise Distribution of the Email ID

From Table 4.16, The finding reveals that aided schools have the highest adoption of personal email IDs among students (76.9%), followed by government schools (74.9%) and private schools (71.8%), indicating widespread use across school types and emphasizing the importance of email for communication and educational purposes among students.

Type of School-wise Distribution of Digital Devices Used per Day

From Table 4.17, the finding showed that in aided schools, a significant portion of students allocate their daily digital device usage as follows: 27.3% spend 1 to 2 hours, 16.6% use devices for 2 to 4 hours, and 28.5% engage for 30 minutes to 1 hour. Government schools show a similar pattern with 26.3% using devices for 1 to 2 hours, 28.7% for 30 minutes to 1 hour, and 18.6% for less than 30 minutes daily. Meanwhile, in private schools, 28.2% of students use devices for 1 to 2 hours daily, 27.7% for 30 minutes to 1 hour, and 15.4% for 2 to 4 hours.

Type of School-wise Distribution of Excessive Screen Time

From Table 4.18, the findings showed In aided schools, the distribution of excessive screen time shows that 24.0% of students spend up to 30 minutes, 22.8% spend 30 minutes to 1 hour, and 19.6% spend 1 to 2 hours on screens. Government schools report that 29.9% of students spend up to 30 minutes, 24.1% spend 30 minutes to 1 hour, and 19.9% spend 1 to 2 hours on screens. Private schools indicate that 24.2% of students spend up to 30 minutes, 21.5% spend 30 minutes to 1 hour, and 19.5% spend 1 to 2 hours on screens.

Type of School wise Distribution of courses related to ICT

From Table 4.19, In aided schools, 40.9% offer courses related to ICT, while 59.1% do not, Government schools show a nearly equal distribution, with 48.1% offering ICT courses and 51.9% not offering them, Among private schools, 46.9% provide ICT courses, while 53.1% do not.

Locality-wise Distribution of Internet access at home

From Table 4.20, the result indicates In Rural Areas, 86.7% of respondents have internet access at home, 13.3% do not have internet access at home. And in Urban Areas, 88.8% of respondents have internet access at home, 11.2% do not have internet access at home. This indicates that a higher percentage of people in both rural and urban areas have internet access at home, with urban areas showing a slightly higher access rate compared to rural areas.

Locality-wise Distribution of Email ID

From Table 4.21, the results indicate that a higher percentage of respondents in urban areas (75.5%) have personal email IDs compared to those in rural areas (72.9%), highlighting slightly greater digital connectivity in urban settings.

Locality-wise Distribution of Digital Devices Used per day

From Table 4.22, The findings show that in rural areas, 29.5% of respondents use digital devices for 30 minutes to 1 hour daily, and 24.0% use them for 1 to 2 hours, indicating moderate digital engagement. In contrast, urban areas have higher usage for 1 to 2 hours (27.8%) and 30 minutes to 1 hour (28.2%), with more varied usage patterns including longer durations of device use compared to rural areas.

Locality-wise Distribution of Excessive Screen Time

From Table 4.23, In rural areas, most respondents spend up to 30 minutes (35.8%) or between 30 minutes to 1 hour (26.1%) on excessive screen time, with fewer spending longer durations like 1 to 2 hours (18.6%). Urban areas show a similar trend, with the majority spending up to 30 minutes (25.8%) or between 30 minutes to 1 hour (22.7%), and a significant portion spending 1 to 2 hours (20.4%) on excessive screen time.

Locality-wise Distribution of courses related to ICT

From Table 4.24, In rural areas, 52.7% of respondents have access to ICT courses, indicating a strong interest and participation in ICT education. Conversely, in urban areas, a lower percentage (45.3%) reported access to these courses, suggesting comparatively less engagement in ICT education among urban residents.

State-wise Distribution of Internet access at home

From Table 4.25, the result indicates that Mizoram stands out with the highest percentage of households having internet access at home at 94.9%. Delhi and Kerala also demonstrate notable rates of 86.0% and 90.7% respectively. Conversely, states like Andaman and Nicobar Islands and Arunachal Pradesh show significant but comparatively lower percentages of internet access at 90.8% and 91.3% respectively, which are below the national average.

State-wise Distribution of Availability of personal email ID

From Table 4.26, the result indicates Mizoram leads with the highest percentage of students (68.5%) having personal email IDs, followed by Delhi (73.9%) and Kerala (88.2%), while states like Dadra and Nagar Haveli and Daman and Diu, Gujarat, and Sikkim show relatively lower adoption rates.

State-wise Distribution of usage of digital devices per day

From the table 4.27, the findings reveal that in Andaman and Nicobar Islands, 29.5% of students use digital devices for less than 30 minutes daily, while in Andhra Pradesh, 32.4% use them for 30 minutes to 1 hour daily, and in Arunachal Pradesh, 30.7% use them for 1 to 2 hours daily. Across states, predominant usage patterns are observed in these moderate time ranges, with fewer students using devices for more than 4 hours or infrequently.

State-wise Distribution of consideration of hours as excessive screen time

From Table 4.28, the result indicates that Arunachal Pradesh and Gujarat for 1 to 2 hours, Odisha and Kerala for 2 to 4 hours, and Mizoram and Haryana for 30 minutes to 1 hour daily, while some states like Dadra and Nagar Haveli and Daman and Diu, Puducherry, and Lakshadweep show a majority of students not using digital devices daily.

State-wise Distribution of courses related to ICT

From above table 4.29, the result indicates the majority of students in Andaman and Nicobar Islands (60.7%), Delhi (50.5%), Punjab (60.2%), Himachal Pradesh (57.4%), Ladakh (66.7%), and Lakshadweep (83.3%) use ICT.

Analysis of data with regard to awareness about cyber safety and security

H_{01}: There is no significant difference between the mean scores for cyber safety and security awareness among students with and without access to the internet at home.

From Table 4.30 it is evident that

- There is a significant difference in cyber safety awareness scores between students who have internet access at home and those who do not.
- Students with internet access at home tend to have higher average scores in cyber safety awareness compared to those without internet access.

H_{02}: There is no significant difference between the mean scores for cyber safety and security awareness among students with ownership of email ID and those without it.

From Table 4.31, the finding showed that,

- Students who have an email ID show a significant difference in cyber safety awareness scores compared to those who do not.
- On average, students with an email ID tend to have slightly higher scores in cyber safety awareness than those without an email ID.

H_{03}: There is no significant difference in the total awareness scores between students who have participated in ICT courses and those who have not.

From Table 4.32 the findings showed that the students who participated in ICT courses showed a significant difference in cyber safety awareness scores compared to those who did not.

- On average, students who did not participate in ICT courses tend to have higher scores in cyber safety awareness than those who did participate.

H_{04}: There is no significant difference in the total awareness scores between individuals who have access to digital devices at home and those who do not.

From Table 4.33 the findings showed that the students who have access to digital devices at home show a significant difference in cyber safety awareness scores compared to those who do not.

- On average, students with access to digital devices at home tend to have higher scores in cyber safety awareness than those without access.

H_{05}: There is no significant difference in the total awareness scores between individuals who use their devices and those who do not.

From Table 4.34 the findings showed that students who have availability of their device show a significant difference in cyber safety awareness scores compared to those who do not.

- On average, students who do not have availability of their devices tend to have higher scores in cyber safety awareness than those who do have availability.

H_{06}: There is no significant difference in the total awareness scores between individuals who have a social media account and those who do not.

From Table 4.35 the findings showed that.

- The obtained t value of 20.34 indicates a significant difference in cyber safety and security awareness scores between students who have their social media accounts and those who do not ($p < 0.01$).
- Therefore, the null hypothesis, suggesting no difference in awareness scores based on social media account ownership, is rejected in favor of the alternate hypothesis. Students who do not have a social media account have a higher average score in cyber safety awareness (194.92) compared to those who do have one (190.88).

H_{07}: There is no significant difference between the mean scores for cyber safety and security awareness among students and their locality with their dimensions.

The findings showed that Urban secondary students show significantly higher awareness scores on cyber safety and security compared to rural students. This disparity suggests a potential need for targeted interventions to enhance cyber safety awareness among rural secondary students to bridge the gap observed with their urban counterparts.

H_{08}: There is no significant difference between the mean scores for cyber safety and security awareness among students and their gender with their dimensions.

The finding showed that,

- The obtained F value of 343.80 is significant at the 0.01 level, indicating a significant difference in cyber safety and security awareness among genders.
- Therefore, the null hypothesis, suggesting no difference in awareness scores between genders, is rejected in favor of the alternate hypothesis. Gender differences play a significant role in cyber safety awareness, with substantial variations observed between different gender groups.

H_{09}: There is no significant difference between the mean scores for cyber safety and security awareness among students and their standard with their dimensions.

The finding showed that the F value of 186.72, significant at the 0.01 level, shows a notable difference in cyber security awareness among students across different educational standards. This rejects the idea of no differences and supports that awareness levels vary significantly based on the standard of study.

H_{10}: There is no significant difference between the mean scores for cyber safety and security awareness among students and their type of school with their dimensions.

The findings showed that the F value of 583.82, significant at the 0.05 level, reveals a significant difference in cyber safety and security awareness between types of school. This supports the alternate hypothesis, indicating that awareness levels vary significantly between males and females, with females generally demonstrating higher awareness.

5.14. Recommendations and Implications of the Study

The study's finding is meaningful only when it has an educational implication. A few implications of this study are put forth.

- Emphasizing the importance of specific interventions to ensure gender equality and support for both boys and girls in secondary education, as well as incorporating cyber safety and security awareness to prepare them for the digital age.
- Increasing digital literacy and cyber safety awareness among students in both rural and urban regions to ensure safe and effective internet use.
- Enhanced Curriculum Integration: Comprehensive Integration of internet safety and security elements into the existing school curriculum should be initiated. This should include subjects ranging from basic to complex, such as safe surfing behaviors, identifying phishing attempts, the necessity of strong passwords, and social media privacy settings.
- Interactive Workshops: frequent workshops and interactive sessions with cyber security professionals to bring students up to date on the most recent cyber risks and defensive measures should be organized by the schools.
- More ICT courses are required nation-wide since many students are yet to participate any ICT related courses
- The CSSA vary significantly among students who participated in ICT courses and did not participate. Hence CSSA can be improved if we provide ICT training to students with special focus on Cyber Safety and Security.
- Similarly it was found that the CSSA among students having and not having social media accounts varies and those using social media accounts seem to be less aware about CSS. This is highlighting their vulnerability in cyber space and needs to be addressed with priority.
- The screen time of majority of students (duration of use of devices per day) seems to be more than the commonly approved limit of 1-2 hrs and hence need to be addressed for their overall health
- The overall CSSA was found to be high for class 12 students. Hence it is required to give more focus on class 9, 10 and 11 students since lack of awareness may keep them vulnerable in cyberspace.
- With regard to CSSA, it was found that the government school students are having less awareness, and it clearly highlights the training needs of students belonging to govt schools.

Proposed Activities and Developed Student's Handbook

The study's findings, which indicate a lack of awareness regarding cyber safety and security among secondary students (Classes IX through XII), highlight the need for comprehensive interventions. In addition to advocating cyber safety-related student activities, including workshops on recognizing online threats and practical exercises on safe internet practices, the study might advocate for the creation of a student handbook. This handbook could be used as a guide for students, providing practical suggestions and tools for navigating the digital landscape securely, understanding privacy settings, identifying cyber risks such as phishing and cyberbullying, and responding to online occurrences successfully.

5.15. Suggestions for Further Research

Every study has its limitations and delimitations. It is, therefore, desired that similar studies should be conducted after overcoming the limitations. The following insights on further research that could be conducted are presented below:

- Investigate how parents' and teachers' knowledge and involvement influence students' awareness and practices regarding cyber safety.
- Evaluate the effectiveness of integrating cyber safety education into the standard school curriculum.
- Incorporating interactive workshops and practical activities to improve cyber security awareness among secondary students.

REFERENCES

Ahmad, N. A., & Othman, N. (2019). View of Information Privacy Awareness Among Young Generation in Malaysia. *Journal of Science, Technology and Innovation Policy*, *5*(2), 1–10. https://jostip.utm.my/index.php/jostip/article/view/41/41

Ahmad, N., Laplante, P. A., Defranco, J. F., & Kassab, M. (2022). A Cybersecurity Educated Community. *IEEE Transactions on Emerging Topics in Computing*, *10*(3), 1456–1463. https://doi.org/10.1109/TETC.2021.3093444

Ahmed, A. A., Elmi, A. H., Abdullahi, A., & Ahmed, A. Y. (2023). Cybersecurity awareness among university students in Mogadishu: a comparative study. *Indonesian Journal of Electrical Engineering and Computer Science*, *32*(3), 1580–1588. https://doi.org/10.11591/ijeecs.v32.i3.pp1580-1588

Alammari, A., Sohaib, O., & Younes, S. (2022). Developing and evaluating cybersecurity competencies for students in computing programs. *PeerJ Computer Science*, *8*. https://doi.org/10.7717/PEERJ-CS.827

AlDaajeh, S., Saleous, H., Alrabaee, S., Barka, E., Breitinger, F., & Raymond Choo, K. K. (2022). The role of national cybersecurity strategies on the improvement of cybersecurity education. *Computers and Security*, *119*. https://doi.org/10.1016/j.cose.2022.102754

Aldosari, F. F., Aldaihan, M. A., & Alhassan, R. A. (2020). Availability of ISTE Digital Citizenship Standards Among Middle and High School Students and Its Relation to Internet Self-Efficacy. *Journal of Education and Learning*, *9*(5), 59. https://doi.org/10.5539/jel.v9n5p59

Alfalah, A. A. (2023). The role of Internet security awareness as a moderating variable on cyber security perception: Learning management system as a case study. *International Journal of Advanced and Applied Sciences*, *10*(4), 136–144. https://doi.org/10.21833/ijaas.2023.04.017

Aljohni, W., Elfadil, N., Jarajreh, M., & Gasmelsied, M. (2021). Cybersecurity Awareness Level: The Case of Saudi Arabia University Students. *International Journal of Advanced Computer Science and Applications*, *12*(3), 276–281. https://doi.org/10.14569/IJACSA.2021.0120334

Alqahtani, M. A. (2022). Factors Affecting Cybersecurity Awareness among University Students. *Applied Sciences (Switzerland)*, *12*(5). https://doi.org/10.3390/app12052589

Alsharida, R. A., Al-rimy, B. A. S., Al-Emran, M., & Zainal, A. (2023). A systematic review of multi perspectives on human cybersecurity behavior. *Technology in Society*, *73*. https://doi.org/10.1016/j.techsoc.2023.102258

Annabelle, L. (2019). *Why is methodology important in research?* Retrieved from https://www.quora.com/Why-is-methodology-important-in-research

Bagchi, B. K. (2017). *Why is methodology important in research?* Retrieved from https://www.quora.com/Why-is-methodology-important-in-research

Baraba, A., & Tomaš, S. (2022). Online safety awareness of elementary school students from Croatian rural and urban areas. *St Open, 3*, 1–8. https://doi.org/10.48188/so.3.7

Baraković, S., & Baraković Husić, J. (2023). Impact of Covid-19 Pandemic Circumstances on Cyber Hygiene of University Students. *International Journal of Human-Computer Interaction*. https://doi.org/10.1080/10447318.2023.2247577

CIET. (2021). *Be Safe in the Cyber World*. NCERT. https://ciet.ncert.gov.in/storage/app/public/files/14/cybersafety/Cyber_safety_for_Students_new.pdf

Coolican, H. (2004). *Research methods and statistics in psychology*. New York, NY: Psychology Press.

Dhaka, S. (2020). Cyber Crime Awareness among Senior Secondary School Students in District Meerut. *Innovation The Research Concept*, *5*(2), 5–8.

Dorasamy, M., Kaliannan, M., Jambulingam, M., Ramadhan, I., & Sivaji, A. (2021). Parents' awareness on online predators: Cyber grooming deterrence. *Qualitative Report*, *26*(11), 3685–3723. https://doi.org/10.46743/2160-3715/2021.4914

Durak, G., Cankaya, S., Yünkül, E., Taylan, U., Erten, E., & Akpinar, S. (2017). Influence of a Game-Based Application on Secondary School Students' Safe Internet Use. *European Journal of Education Studies*, *3*(10), 22. https://doi.org/10.5281/zenodo.1012416

Ellala, Z. K., AL-Tkhayneh, K. M., & AlKhatib, R. N. (2023). The Extent of Awareness of Cyber Security Among the Superior and Ordinary Students in the Faculty of Education in Al Ain University. In *Studies in Systems, Decision and Control* (Vol. 488, pp. 134–144). Springer Science and Business Media Deutschland GmbH. https://doi.org/10.1007/978-3-031-39158-3_12

Erdoğdu, F., Gökoğlu, S., & Kara, M. (2021). "What about users?": Development and validation of the mobile information security awareness scale (MISAS). *Online Information Review*, *45*(2), 406–421. https://doi.org/10.1108/OIR-04-2020-0129

Erendor, M. E., & Yildirim, M. (2022). Cybersecurity Awareness in Online Education: A Case Study Analysis. *IEEE Access*, *10*, 52319–52335. https://doi.org/10.1109/ACCESS.2022.3171829

Fatokun Faith, B., Hamid, S., Norman, A., Fatokun Johnson, O., & Eke, C. I. (2020). Relating Factors of Tertiary Institution Students' Cybersecurity Behavior. *2020 International Conference in Mathematics, Computer Engineering and Computer Science, ICMCECS 2020*, 0–5. https://doi.org/10.1109/ICMCECS47690.2020.246990

Good, C. V. (1972). Dictionary of education. McGraw-Hill. Retrieved from https://www.jstor.org/stable/20495320

Huraj, L., Lengyelfalusy, T., Hurajová, A., & Lajčin, D. (2023). Measuring Cyber Security Awareness: A Comparison between Computer Science and Media Science Students. *TEM Journal*, *12*(2), 623–633. https://doi.org/10.18421/TEM122-05

Jalil, M., Ali, N. H., Yunus, F., Zaki, F. A. M., Hsiung, L. H., & Almaiah, M. A. (2024). Cybersecurity Awareness among Secondary School Students Post Covid-19 Pandemic. *Journal of Advanced Research in Applied Sciences and Engineering Technology*, *37*(1), 115–127. https://doi.org/10.37934/araset.37.1.115127

Jian, N. J., & Kamsin, I. F. B. (2021). Cybersecurity Awareness Among the Youngs in Malaysia by Gamification. *Proceedings of the 3rd International Conference on Integrated Intelligent Computing Communication & Security (ICIIC 2021)*, *4*(Iciic), 487–494. https://doi.org/10.2991/ahis.k.210913.061

Kelley, K. (2023). What is Cybersecurity and Why It is Important? simplilearn. https://www.simplilearn.com/tutorials/cyber-security-tutorial/what-is-cyber-security. Retrieved on 30/01/24.

Kesharwani, S. (2020). *14C A New Cyber Initiative- By Government of India in 2020*. *6*, 25–31.

Khader, M., Karam, M., & Fares, H. (2021). Cybersecurity awareness framework for academia. *Information (Switzerland)*, *12*(10), 1–20. https://doi.org/10.3390/info12100417

Khalid, F., & El-Maliki, T. (2020). Teachers' experiences in the development of digital storytelling for cyber risk awareness. *International Journal of Advanced Computer Science and Applications*, *2*, 186–191. https://doi.org/10.14569/ijacsa.2020.0110225

Khan, N. F., Ikram, N., Saleem, S., & Zafar, S. (2023). Cyber-security and risky behaviors in a developing country context: a Pakistani perspective. In *Security Journal* (Vol. 36, Issue 2). Palgrave Macmillan UK. https://doi.org/10.1057/s41284-022-00343-4

Klein, G., Zwilling, M., & Lesjak, D. (2020). A comparative study in Israel and Slovenia regarding the awareness, knowledge, and behavior regarding cyber security. In *Responsible AI and Ethical Issues for Businesses and Governments* (pp. 128–147). IGI Global. https://doi.org/10.4018/978-1-7998-4285-9.ch007

Koyuncu, M., & Pusatli, T. (2019). Security Awareness Level of Smartphone Users: An Exploratory Case Study. *Mobile Information Systems*, *2019*. https://doi.org/10.1155/2019/2786913

Kritzinger, E. (2020). Improving cyber safety maturity of South African schools. *Information (Switzerland)*, *11*(10), 1–17. https://doi.org/10.3390/info11100471

Lobe, B., Simoes, J. A., Zaman, B., & L. Haddon. (2009). Research with children. In: S. Livingstone, *Kids online. Opportunities and risks for children*, 31-40. Bristol: The Policy Press.

Ma, S., Wang, Y., Shu, Z., Duan, Z., & Sun, L. (2023). Development and validation of Internet literacy scale for high school students. *Education and Information Technologies*, *0123456789*. https://doi.org/10.1007/s10639-023-11641-8

Macaulay, P. J. R., Boulton, M. J., Betts, L. R., Boulton, L., Camerone, E., Down, J., Hughes, J., Kirkbride, C., & Kirkham, R. (2020). Subjective versus objective knowledge of online safety/dangers as predictors of children's perceived online safety and attitudes

towards e-safety education in the United Kingdom. *Journal of Children and Media*, *14*(3), 376–395. https://doi.org/10.1080/17482798.2019.1697716

Mai, P. T., & Tick, A. (2021). Cyber security awareness and behavior of youth in smartphone usage: A comparative study between university students in Hungary and Vietnam. *Acta Polytechnica Hungarica*, *18*(8), 67–89. https://doi.org/10.12700/APH.18.8.2021.8.4

Martin, F., Gezer, T., Anderson, J., Polly, D., & Wang, W. C. (2021). Examining Parent's Perception on Elementary School Children Digital Safety. *Educational Media International*, *58*(1), 60–77. https://doi.org/10.1080/09523987.2021.1908500

Masenya, T. M. (2023). Awareness and knowledge of cyber ethical behavior by students in higher education institutions in South Africa. In *Handbook of Research on Cybersecurity Risk in Contemporary Business Systems* (pp. 33–48). IGI Global. https://doi.org/10.4018/978-1-6684-7207-1.ch002

McCombes, S. (2020). *Descriptive research*. Scribbr. Retrieved from https://www.scribbr.com

MHRD. (2020). National Education Policy 2020. Government of India. https://www.education.gov.in/sites/upload_files/mhrd/files/NEP_Final_English_0.pdf

MoE. (2021). Report on Unified District Information System for Education Plus (UDISE+). In *Goi*. https://dashboard.udiseplus.gov.in/#/home

Mohammed, M., & Bamasoud, D. M. (2022). The Impact of Enhancing Awareness of Cybersecurity on Universities Students: A Survey Paper. *Journal of Theoretical and Applied Information Technology*, *100*(15), 4756–4766. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85138808067&partnerID=40&md5=f5409059905f855f94029d0526d10d6b

Mousa, S. (2019). Cyber security: exploring awareness among University Students at a Public Educational Institution. *International Journal of Innovative Research and Knowledge*, *4*(5), 88–97. https://www.semanticscholar.org/paper/Cyber-Security-%3A-Exploring-Awareness-among-Students-Mousa/b49f62de4dd6edafc0fae4deabf39404c5ce73c5

Musharraf, S., Bauman, S., Anis-ul-Haque, M., & Malik, J. A. (2019). General and ICT self-efficacy in different participants roles in cyberbullying/victimization among Pakistani university students. *Frontiers in Psychology*, *10*(MAY), 1–11. https://doi.org/10.3389/fpsyg.2019.01098

NCF. (2023). National Curriculum Framework for School Education 2023. In the National *Council of Educational Research and Training*. https://dsel.education.gov.in/sites/default/files/NCF2023.pdf

NEP. (2020). National Education Policy 2020. *Economic and Political Weekly*, *55*(31), 4L. https://doi.org/10.1201/9781003254942-12

Nicolaidou, I., & Venizelou, A. (2020). Improving children's E-safety skills through an interactive learning environment: A quasi-experimental study. *Multimodal Technologies and Interaction*, *4*(2). https://doi.org/10.3390/mti4020010

Nkechi, L., Harcourt, P., & State, R. (2020). Achieving Cyber Safety in Junior Secondary Schools in Rivers State, Nigeria. *The International Journal of Humanities & Social Studies*, *8*(4), 141–147.

Omar, N. S., Foozy, C. F. M., Hamid, I. R. A., Hafit, H., Arbain, A. F., & Shamala, P. (2021). Malware Awareness Tool for Internet Safety using Gamification Techniques. *Journal of Physics: Conference Series*, *1874*(1). https://doi.org/10.1088/1742-6596/1874/1/012023

Podila, L. M., Bandreddi, J. P., Campos, J. I., Niyaz, Q., Yang, X., Trekles, A., Czerniak, C., & Javaid, A. Y. (2020). Practice-oriented smartphone security exercises for developing a cybersecurity mindset in high school students. *Proceedings of 2020 IEEE International Conference on Teaching, Assessment, and Learning for Engineering, TALE 2020*, 303–310. https://doi.org/10.1109/TALE48869.2020.9368440

Prathyush, N. G. P., & Kumar, N. G. P. D. (2022). A Study of Cybersecurity and its Role in Information Technology along with the Emerging Trends and Latest Technologies. *International Journal of Advanced Research in Science, Communication and Technology*, 854–858. https://doi.org/10.48175/ijarsct-7576

Quinn, S. (2013). *The role of social networking site use in feelings of belonging among 9 to 13-year-olds.* University of York, Psychology, Retrieved from http://etheses.whiterose.ac.uk/5700/

Quyen, D., & Lien, N. H. (2022). Literature review of research in the area of digital safety competency for school-age students and the prospect of digital safety education in Vietnam. *Vietnam Journal of Educational Sciences*, *18*(3), 40–51.

Rahman, N. A. A., Sairi, I. H., Zizi, N. A. M., & Khalid, F. (2020). The importance of cybersecurity education in school. *International Journal of Information and Education Technology*, *10*(5), 378–382. https://doi.org/10.18178/ijiet.2020.10.5.1393

Raju, R., Rahman, N. H. A., & Ahmad, A. (2022). Cyber Security Awareness In Using Digital Platforms Among Students In A Higher Learning Institution. *Asian Journal of University Education*, *18*(3), 756–766. https://doi.org/10.24191/ajue.v18i3.18967

Rakhmatov, D., & Akhatov, A. (2020). *Factors of cybercrime and cyber ethics: problems and prospects*. *1*, 227–235.

Saxena, A. (2023). Importance of cyber security: Benefits and Disadvantages. sprinto. https://sprinto.com/blog/importance-of-cyber-security/ Retrieved on 30/01/24.

Shah, P., & Agarwal, A. (2023). Cyber Suraksha: a card game for smartphone security awareness. *Information and Computer Security*, *31*(5), 576–600. https://doi.org/10.1108/ICS-05-2022-008

Sussman, L. L. (2023). Everyday Cyber Safety for Students. In *Studies in Computational Intelligence* (Vol. 1080, pp. 3–24). Springer Science and Business Media Deutschland GmbH. https://doi.org/10.1007/978-3-031-21199-7_1

Tomczyk, & Eger, L. (2020). Online safety as a new component of digital literacy for young people. *Integration of Education*, *24*(2), 172–184. https://doi.org/10.15507/1991-9468.099.024.202002.172-184

Tsimtsiou, Z., Drosos, E., Drontsos, A., Haidich, A.-B., Dantsi, F., Sekeri, Z., Dardavesis, T., Nanos, P., & Arvanitidou, M. (2021). Raising awareness on cyber safety: Adolescents' experience of primary healthcare professional-led, school-based, multi-centre intervention. *International Journal of Adolescent Medicine and Health*, *31*(6). https://doi.org/10.1515/ijamh-2017-007

Tsokoto, T., Mhloza, V., & Kangara, C. C. (2019). A Strategy To Enhance E-Safety Among First Year Students at Zimbabwean Universities. *Journal of Governance and Development*, *15*(2), 67–85.

Wahid, S. D. M., Buja, A. G., Hasrol Jono, M. N. H., & Aziz, A. A. (2021). Assessing the influential factors of cybersecurity awareness in Malaysia during the pandemic outbreak: A structural equation modelling. *International Journal of Advanced Technology and Engineering Exploration*, *8*(74), 73–81. https://doi.org/10.19101/IJATEE.2020.S1762116

Wei-Kocsis, J., Sabounchi, M., Mendis, G. J., Fernando, P., Yang, B., & Zhang, T. (2023). Cybersecurity Education in the Age of Artificial Intelligence: A Novel Proactive and Collaborative Learning Paradigm. *IEEE Transactions on Education*, 0–1. https://doi.org/10.1109/TE.2023.3337337

Zulqadri, D. M., Mustadi, A., & Retnawati, H. (2022). Digital Safety During Online Learning: What We Do to Protect Our Student? *Jurnal Iqra': Kajian Ilmu Pendidikan*, *7*(1), 178–191. https://doi.org/10.25217/ji.v7i1.1746