DATA PRIVACY AND SECURITY:

A CASE STUDY OF TEXAS COLLEGE

A Bachelor Research Paper submitted in partial fulfilment of the requirement for the internal evaluation

BACHELOR OF INFORMATION TECHNOLOGY

By

BIKRAM ROKAYA

LC00017001368

At the

Texas College of Management and IT

Lincoln University College

Faculty of Computer Science and Multimedia System

17th September, 2023

Acknowledgement

I would like to express my sincere gratitude and appreciation to my faculty supervisor Mr. Saroj Dhital, for his patience, guidance, insightful feedback and support. I am also deeply indebted to the head of the BIT department, Dr. Suman Thapaliya, on his continuous encouragement and supervision throughout this academic endeavor. Thank you to the responder, who so generously took time out of their schedules to participate in my research and make this Research Paper possible.I would like thank to all honorable teachers as well as staff members and my friends of Texas College of Management & IT (TCMIT).The department's commitment to academic excellence and its continuous efforts to enhance the learning experience have played a significant role in shaping our overall understanding of the Research Process.

Lastly, thank you to my parents, for your endless support who have always stood behind me, and this was no exception.

With Regards

Bikram Rokaya

LCID: LC00017001368

Executive Summary

This study explores the complexities of data privacy and security within the context of personal interactions among college mates, teachers, and other friends. The primary objective was to gain insights into the challenges and opportunities related to safeguarding sensitive information in the context of social and academic relationships.

Through surveys and observations, this study revealed several noteworthy findings. Firstly, individuals within these close-knit circles express varying levels of awareness concerning data privacy and security. While some are vigilant about protecting their personal information, others may inadvertently expose sensitive data during social interactions.

The advent of digital communication platforms and social media has revolutionized how college mates, teachers, and friends interact. These tools offer convenience but also pose inherent risks such as data leaks, identity theft, and privacy breaches. Participants in this study highlighted the importance of setting clear boundaries and educating themselves on best practices for secure online communication.

Despite these challenges, the study revealed a strong sense of trust and camaraderie among individuals within these circles. Friends and acquaintances often play a pivotal role in alerting one another to potential risks and providing support in times of need. However, there is a collective desire for increased awareness and proactive measures to protect personal data and privacy.

Table of contents

Acknowledgement ii

Executive Summary iii

Chapter 1: Introduction 6

1.1 Background of the Study **6**

1.2 Problem Statement **6**

1.3 Objectives of the Study **7**

1.4 Research Questions **8**

1.5 Scope and Significance of the Study **9**

1.6 Limitations of the Study **10**

Chapter 2 Literature Review 11

2.1 Data Privacy and Security **11**

2.2 Literature Review on Personal Data Online and Data Privacy **11**

2.3 Privacy Prevention of Big Data Applications **12**

2.4 Data Privacy Issues and Challenges **13**

2.5 Data Security in Cloud Computing 14

2.6 Literature Findings **14**

2.6.1 Concerns About Data Privacy: **14**

2.6.2 Factors Influencing Willingness to Share Personal Information **15**

2.6.3 Demographics and Data Privacy Attitude **15**

2.6.4 Storage of Important Data/Files **15**

2.6.5 Trust in Organizations with Personal Data **15**

Chapter 3 Research Methods 16

3.1 Research Design **16**

3.2 Population and Sample **16**

3.3 Sampling Techniques **16**

3.4 Data **17**

3.4.1 Nature of data 17

3.4.2 Source of data 17

3.5 Method of Analysis **18**
Chapter 4 Analysis and Result 19
4.1 Quantitative Analysis: **19**
Chapter 5 Discussion, Conclusions and Implications 25
5.1 Discussion **25**
5.2 Conclusions **26**
5.3 Implications **26**
References 28
Appendices 29
Appendix: Form Questions **29**

List of Figures

Figure 1 Awarness of Data Privacy 19
Figure 2 Storage of important file 20
Figure 3 preferred web browser 21
Figure 4 Software update frequency 22
Figure 5 Safety of Sharing Personal Data Publicly 23

Chapter 1: Introduction

1.1 Background of the Study

Data privacy and security are paramount in the digital era, where the rapid proliferation of data and increasing cyber threats demand vigilant protection. Data privacy entails safeguarding personal information from unauthorized access or disclosure, while data security focuses on ensuring data integrity, confidentiality, and availability. These concepts are essential for upholding individuals' rights, preventing identity theft, and fostering trust in digital services. Additionally, organizations must prioritize data protection to mitigate legal repercussions, financial losses, and reputational damage associated with data breaches. Key principles include obtaining informed consent, minimizing data collection, and purpose limitation. The landscape is shaped by stringent data privacy laws as well as evolving technologies such as, AI, and quantum computing. As threats continue to evolve, best practices like security audits, employee training, and incident response plans are critical. Balancing privacy with data utility and addressing global data transfer challenges are ongoing challenges, while emerging trends like privacy-enhancing technologies and data ethics promise to shape the future of data privacy and security.

1.2 Problem Statement

In an increasingly digital and interconnected world, the paramount issue of data privacy and security poses significant challenges and concerns. The rapid expansion of data collection, storage, and sharing has exposed individuals and organizations to a multitude of threats, ranging from cyberattacks and data breaches to unauthorized access and misuse of personal information. These threats not only compromise the confidentiality, integrity, and availability of data but also erode trust in digital services and have far-reaching legal and financial implications.

The problem at hand revolves around the need to strike a delicate balance between harnessing the benefits of data-driven technologies and safeguarding the privacy and security of individuals and their sensitive information. Existing regulations and standards, such as the General Data Protection Regulation (GDPR) and the California Consumer

Privacy Act (CCPA), have laid out essential guidelines for data protection, but compliance remains a significant challenge for organizations globally.

Addressing this multifaceted problem requires a comprehensive understanding of data privacy and security principles, the development of robust technical and organizational measures, and a proactive approach to staying ahead of evolving threats and regulations. Finding effective solutions that ensure data privacy and security without stifling innovation is a pressing concern in our digital age

1.3 Objectives of the Study

The objectives of this study on data privacy and security are:

a) How concerned are people about their data privacy?
b) What factors influence their willingness to share personal information?
c) How do demographics (age, gender, location) affect attitudes toward data privacy?
d) Where people save there important data/file?
e) Do people trust certain types of organizations more with their data than others (e.g., government, social media, healthcare)?

1. To Assess Awareness and Behavior Patterns on Data Privacy and Security:

   Objective: To investigate the awareness levels and behavior patterns of individuals, particularly within the context of personal gadget device usage, social media preferences, password security, data storage practices, and online browsing habits. This objective aims to analyze how these patterns relate to their understanding and implementation of data privacy and security measures.

2. To Evaluate Knowledge and Perceptions of Data Privacy Laws and Regulations: Objective: To assess the participants' knowledge and perceptions regarding data privacy laws and regulations applicable in their country. This objective aims to explore how this knowledge influences their attitudes towards sharing personal data, their trust in third-party entities, and their comfort levels with online privacy. The goal is to investigate whether a greater understanding of legal frameworks promotes a stronger demand for strict rules and regulations to safeguard personal data.

1.4 Research Questions

1. What are the devices you use?
2. Do you use mobile, which one you use?
3. Are you active social media user or not, what you use?
4. Do you know about data privacy, what you know about it?
5. Do you use secure password?
6. Where do you store your important files?
7. Which web browser do you normally use?
8. How often do you use Update for software?
9. Do you have anti-virus software installed on your computer?
10. Which anti-virus software do you use?
11. Do you use firewall software on your computer?
12. Do you trust companies and institutions that they will not misuse your data?
13. How often do you backup your important data to protect it from loss?
14. Are you concerned about the privacy and security of your personal data?
15. Do you use two factor authentication for your account?
16. Have you ever experienced a privacy or security breach related to your personal data?
17. How often do you read privacy policies and terms of service before using a new online service or app?
18. Do you feel that organizations protect your personal data?
19. Are you aware of the types of personal data that organizations collect about you?
20. Do you understand the rights you have regarding your personal data, such as the right to access or delete it?
21. How comfortable are you with sharing personal data in exchange for personalized services or targeted advertising/advertisement?
22. Do you believe that organizations should obtain consent from individuals before collecting or using their personal data?
23. Are you aware of the data privacy laws and regulations in our country?
24. How well do you think organizations communicate their data privacy and security practices to the public?
25. Do you think there should be strict rule and regulation to protect personal data?
26. Do you give access to any website?
27. Do you check the link that you get from other is harmful or safe?
28. Do you think it is safe to share your personal data publicly?
29. Do you use public WIFI ?
30. How often do you review and manage the permissions granted to mobile apps on your device?
31. Have you ever encountered phishing attempts or fraudulent emails?
32. Have you ever used a VPN (virtual private network), for what purpose?
33. Have you shared your ID password of any social media to other?
34. Who is responsible for updating and maintaining security on your computer?
35. Which version of Windows is installed on the computer that you normally use to connect to the Internet?

1.5 Scope and Significance of the Study

This research endeavors to shed light on the critical and ever-evolving landscape of data privacy by addressing five fundamental objectives. Firstly, it seeks to assess the extent to which people are concerned about their data privacy in our interconnected digital world. This understanding forms the bedrock upon which subsequent insights are built, aiding in the evaluation of the urgency and importance of data privacy issues today.

Secondly, the study explores the intricate web of factors that influence individuals' willingness to share personal information. By uncovering the motivations and deterrents behind data sharing, this research provides practical insights for businesses, policymakers, and organizations seeking to navigate the delicate balance between data collection and respecting privacy.

Demographic factors, including age, gender, and location, often play a pivotal role in shaping attitudes and behaviors related to data privacy, constituting the third objective. This exploration will unveil nuanced variations in how different segments of the population perceive and interact with their data, thereby helping identify target audiences for data privacy campaigns and policies.

The fourth objective delves into the diverse array of choices individuals make in storing their important data and files. Given the multitude of storage options available, this aspect of the study provides valuable insights into preferred modes of data storage, which in turn have implications for cybersecurity and data management strategies.

Lastly, examining trust levels in different types of organizations—government entities, social media platforms, healthcare providers, and more—is of significant societal and policy relevance. Understanding where individuals place their trust in data handling can guide the development of regulatory frameworks and inform decisions about data sharing and protection in an increasingly interconnected digital society.

1.6 Limitations of the Study

Survey was done in limited number of peoples like college mates and others friends and friend of friends.The study relies on the accuracy and completeness of the data collected. Data regarding data breaches, security incidents, or privacy compliance may be subject to limitations, including underreporting, incomplete records, or data collection errors. Moreover, respondent bias or incomplete information provided by interviewees or survey participants could affect the comprehensiveness of the findings.

The conclusions are drawn from data collected during a specific timeframe. Given the rapidly evolving nature of cybersecurity threats and technologies, the findings may not fully capture future developments in data privacy and security practices. New threats, regulations, or technologies could emerge after the data collection period, potentially impacting the effectiveness of the strategies discussed in the study.

Chapter 2 Literature Review

2.1 Data Privacy and Security

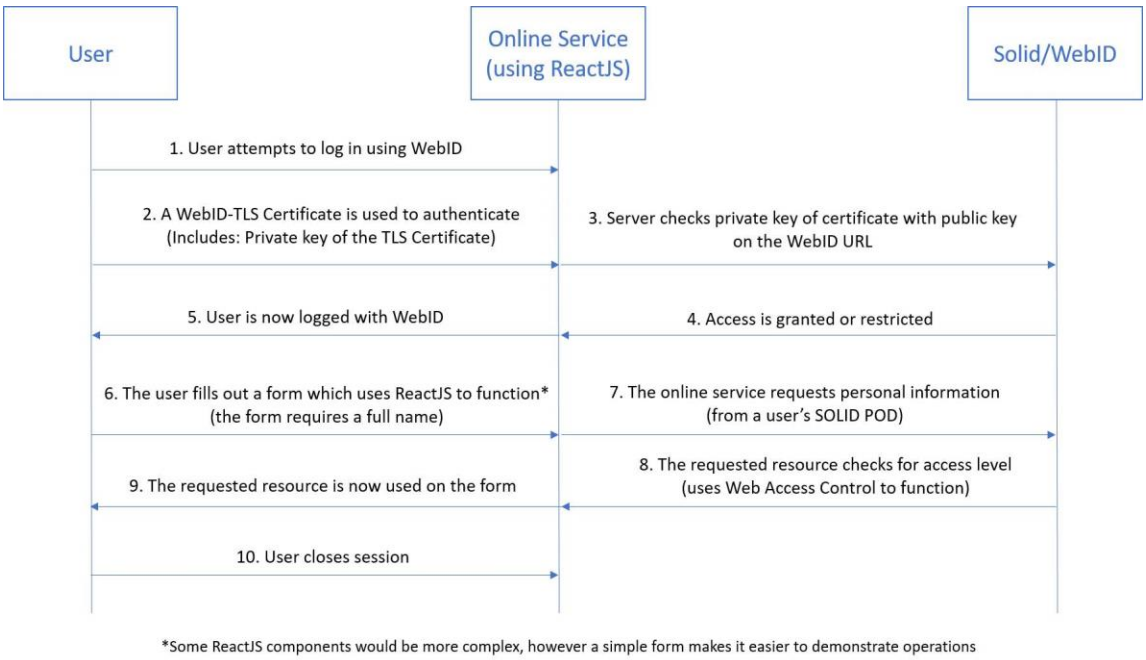
Smart tourism has gained popularity in recent years. While we praise the benefits it brings, we should not neglect the associated challenges of data privacy and security. This study intends to investigate the scope of data privacy and security research on smart tourism by analyzing 38 relevant contributions in multi-disciplinary fields systematically. Historical trends, disciplines, regions, themes, relevance, methods, and theories were analyzed to map out the existing research on data privacy and security in smart tourism. Findings reveal that although relevant studies have grown in frequency in recent years, there is still a lack of attention to tourists' information privacy and security in smart tourism research. Specifically, privacy-based conceptualized studies, theory-driven empirical research, and legal analysis in data protection deserve immediate attention. Tourism scholars should also consider proper methods to raise tourists' data privacy and security awareness and build an ethical relationship between tourists and smart tourism applications.

2.2 Literature Review on Personal Data Online and Data Privacy

This literature review has enabled this project to discover its relevance to find a solution to many apparent issues with the use of personal data and privacy online. It shows that online services need personal data for various reasons, however they are clearly not competent in protecting it; which is what this project is trying to achieve a solution for.

The technologies used set a base to enable users to protect their data online, whilst still being able to use online services. Solid allows online services to communicate with personal data hosted via a pod, they can then use it, but they will not need to be responsible for storing it. Then ReactJS will allow this project to become even more relevant, as many popular online services have been found using ReactJS (Coder Academy, n.d.).

The two technologies will communicate as seen in the diagram below, which is adapted from the official Solid GitHub pages.



2.3 Privacy Prevention of Big Data Applications

This paper focuses on privacy and security concerns in Big Data. This paper also covers the encryption techniques by taking existing methods such as differential privacy, *k*-anonymity, *T*-closeness, and *L*-diversity. Several privacy-preserving techniques have been created to safeguard privacy at various phases of a large data life cycle. The purpose of this work is to offer a comprehensive analysis of the privacy preservation techniques in Big Data, as well as to explain the problems for existing systems. The advanced repository search option was utilized for the search of the following keywords in the search: "Cyber security" OR "Cybercrime") AND (("privacy prevention") OR ("Big Data applications")). During Internet research, many search engines and digital libraries were utilized to obtain information. The obtained findings were carefully gathered out of which 103 papers from 2,099 were found to gain the best information sources to address the provided study subjects. Hence a systemic review of 32 papers from 103 found in major databases (IEEExplore, SAGE, Science Direct, Springer, and MDPIs) were carried out, showing that the majority of them focus on the privacy prediction of Big Data applications

with a contents-based approach and the hybrid, which address the major security challenge and violation of Big Data. We end with a few recommendations for improving the efficiency of Big Data projects and provide secure possible techniques and proposed solutions and model that minimizes privacy violations, showing four different types of data protection violations and the involvement of different entities in reducing their impacts.

Figure 1. The six V's of Big Data.

2.4 Data Privacy Issues and Challenges

we strived to find out the challenges and ethical issues in the stream of data privacy in the present era of the twenty-first century, based on old studies. To review the literature, a range of sources were searched on the topic and fifty-one research papers have been taken as a sample, out of which nine are from USA and India each and eight form Philippines. The present study focuses on empirical studies which were published during the period 2008-2020. Different kinds of journals, magazines, articles, newspaper, websites, etc. have been explored to analyze ancient data for research purpose. During the research, efforts have been made to identify the challenges as well as ethical issues which the researchers have to face during the research process. In the research, it has been founded that there exist a lot of challenges for the data privacy and it becomes very difficult to follow the ethics to maintain the privacy and security of data in this technologydriven era. In the end, based on available data it has been concluded that there is a great need of hard

punishments for those people who misuse the data for their own sake and demoralize those people who make hard efforts to carry out the research and generate new concepts and ideas. So the government should take necessary measures toward data privacy area for security and safety purpose.

2.5 Data Security in Cloud Computing

Cloud computing is an Internet-based computing and next stage in evolution of the internet. It has received significant attention in recent years but security issue is one of the major inhibitor in decreasing the growth of cloud computing. It essentially shifts the user data and application software to large datacenters i e, cloud, which is remotely located, at which user does not have any control and the management of data may not be completely secure. However, this sole feature of the cloud computing introduce many security challenges which need to be resolved and understood clearly. One of the most important and leading is security issue that needs to be addressed. Data Security concerns arising because both user data and program are located in provider premises. In this study, an attempt is made to review the research in this field. The results of review are categorized on the basis of type of approach and the type of validation used to validate the approach.

2.6 Literature Findings

"Data privacy and security" can be identified by examining the existing literature and the current state of knowledge of data privacy and security among peoples, students.

2.6.1 **Concerns About Data Privacy**:

Data privacy concerns have been on the rise globally. High-profile data breaches and scandals have increased public awareness.Surveys consistently show that a majority of people are concerned about the privacy of their personal data online.

2.6.2 Factors Influencing Willingness to Share Personal Information

Trust in the organization or platform collecting the data is a significant factor. People are more willing to share data with entities they trust. Individuals are often willing to share data if they perceive benefits, such as personalized

2.6.3 Demographics and Data Privacy Attitude

Age: Younger individuals are often more willing to share data and may have a higher tolerance for online data collection. Older individuals may be more privacy-conscious.

2.6.4 Storage of Important Data/Files

People use various methods to store important data/files, including cloud storage services (e.g., Google Drive, Dropbox), physical external hard drives, and local storage on devices (e.g., laptops, smartphones)

2.6.5 Trust in Organizations with Personal Data

Trust in organizations varies. Generally, people may trust healthcare providers more with their medical data due to strict privacy regulations. Conversely, social media platforms and tech companies are often viewed with skepticism due to past data misuse incidents. Government organizations' trust levels can vary depending on the country and its data privacy policies.

Chapter 3 Research Methods

3.1 Research Design

For this research, a combination of qualitative and quantitative research designs has been employed. Qualitative research lets me dig deep into the experiences and perceptions of educators and students regarding data privacy and security education at Texas College mates and within other friends group and friends of friends group. This design enables a comprehensive understanding of the human aspects of this story, shedding light on how sharing personal data is influencing the personal life and security.

3.2 Population and Sample

This study encompasses a diverse range of participants from various field including educators (teachers), college mates, friends and friends of friends. The aim is to gather insights from multiple perspectives to provide a holistic view of data privacy and security.

3.3 Sampling Techniques

Sampling techniques are essential in research as they help researchers select a subset of individuals or items from a larger population. The primary goal is to ensure that the chosen sample is representative of the entire population, thereby enabling valid and generalizable results.

Convenience sampling was employed in this research study to collect data from peoples of different field and area. This method was chosen due to its practicality and the accessibility of participants within the study's context. The questionnaire was send as a google form to the applicant who were readily available and willing to participate.

3.4 Data

3.4.1 Nature of data

The data collected for this research is primarily of a quantitative nature, consisting of numerical measurements and structured responses. The data was gathered through a questionnaire that incorporated the following characteristics:

3.4.1.1 Data Type: The data gathered is quantitative, encompassing numerical data and responses to predefined questions.

3.4.1.2 Data Format: The data was collected through a structured questionnaire comprising multiple-choice questions, Likert scale ratings, and a few open-ended text questions.

3.4.1.3 Scale of Measurement: The variables encompassed a range of measurement scales, including nominal (e.g., college affiliation), ordinal (e.g., Likert scale ratings), and interval (e.g., age groups). The sample size of this research included 113 respondents.

3.4.2 Source of data

The data for this research was sourced from college mates of Texas College other friends and friends of friends and relatives ,constituting the target population. The following details describe the source of data:

3.4.2.1 Population: The study's population consists of bachelor's students at Texas College, representing a subset of the broader student community.

3.4.2.2 Sampling Method: Convenience sampling was employed to select participants for the research. This method was chosen due to its practicality and the accessibility of participants within the study's context.

3.4.2.3 Data Collection Procedure: The data collection process involved the electronic administration of the questionnaire. Participants were contacted through email and online platforms and were requested to complete the questionnaire voluntarily.

3.4.2.4 Data Collection Timeframe: Data collection took place over a specific period, spanning from July 2023 to August 2023 during which responses were collected from the selected participants.

3.4.2.4 Ethical Considerations: Ethical considerations were observed throughout the research process. Informed consent was obtained from all participants, ensuring their willingness to participate, and measures were taken to maintain the confidentiality and anonymity of their responses.

3.5 Method of Analysis

In this section, I will outline the method of analysis employed to process and derive insights from the collected data. The data analysis process for this research will be conducted primarily using Microsoft Excel due to its versatility and suitability for both quantitative and qualitative data analysis.

3.5.1 Data Cleaning

The initial step was data cleaning in which I have checked for missing values and data inconsistencies.

3.5.2 Data Visualization

I have choose bar chart for visual representation of data using Microsoft Excel.

Chapter 4 Analysis and Result

Based on the responses collected from the questionnaire, I can draw conclusions by conducting both quantitative and qualitative analyses. Here, I'll present key findings and interpretations in a point-by-point format, combining insights from both data types

4.1 Quantitative Analysis:

4.1.1 Awareness of Data Privacy

The majority of respondents (70 out of 75) demonstrate an understanding of data privacy. This indicates a generally well-informed group concerning the protection and control of personal data. However, it's concerning that a small portion (5 responses) express a lack of awareness about data privacy. This highlights a need for educational efforts to enhance understanding and awareness about safeguarding personal information.

Awareness of Data Privacy		
Options	**Responses**	**Responses (in %)**
Yes	90	78.94736842
No	24	21.05263158
Total	**114**	**100**

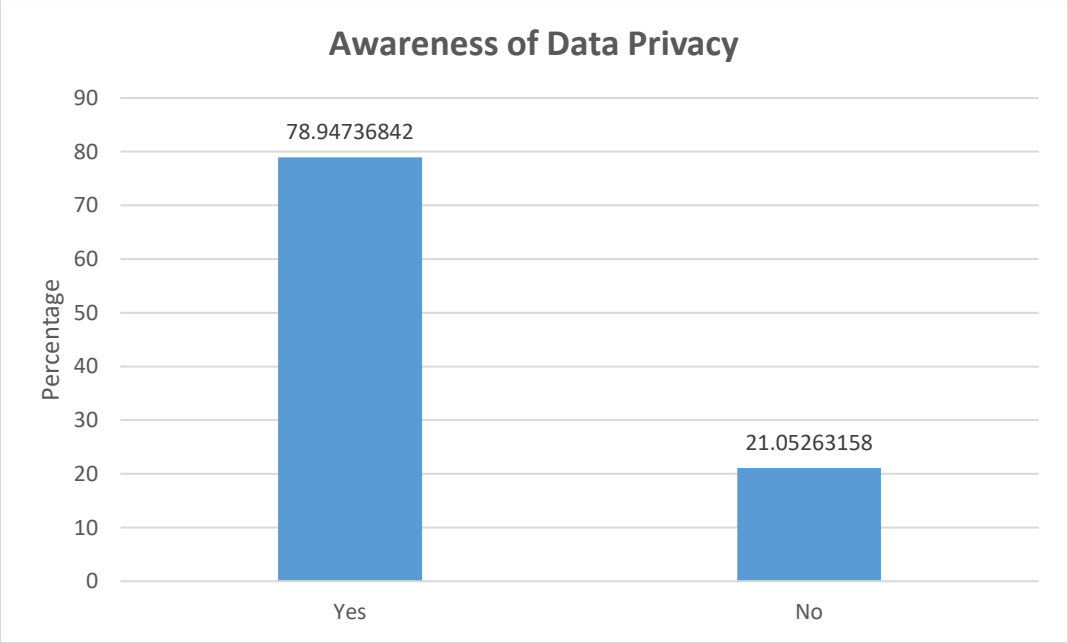


Figure 1 Awarness of Data Privacy

4.1.2 Storage of Important Files

Google Drive emerges as the favored choice for storing important files, with 62 respondents opting for this cloud-based solution. This reflects a trend towards convenient and easily accessible cloud storage. However, a significant number (34 responses) prefer physical storage such as hard drives or pen drives, underscoring a preference for tangible control over data. A notable portion (11 responses) uses other cloud services, indicating a diverse range of storage preferences based on individual needs and preferences.

Storage of Important Files		
Options	**Responses**	**Responses (in %)**
Google Drive	64	56.14035088
Hard Drive	30	26.31578947
Internal Storage	6	5.263157895
Cloud	11	9.649122807
Other	3	2.631578947
Total	**114**	**100**

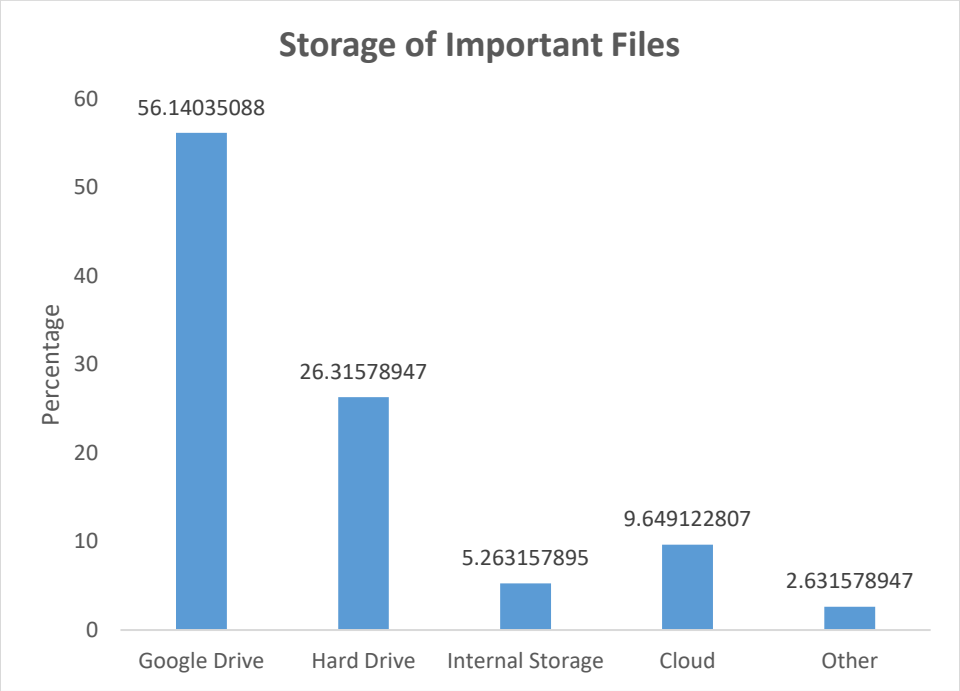


Figure 2 Storage of important file

4.1.3 Preferred Web Browser

Chrome is overwhelmingly the most frequently used web browser, with 104 responses. This indicates its widespread popularity and user comfort within the group. Brave and Mozilla Firefox also have a notable user base, reflecting a preference for alternative browsers. The lower usage of Microsoft Edge and other browsers suggests a dominant presence of Chrome and a need to explore the reasons behind this preference further.

Preferred Web Browser		
Options	**Responses**	**Responses (in %)**
Chrome	80	70.1754386
Brave	16	14.03508772
Mozilla Firefox	13	11.40350877
Microsoft Edge	4	3.50877193
Others	1	0.877192982
Total	**114**	**100**

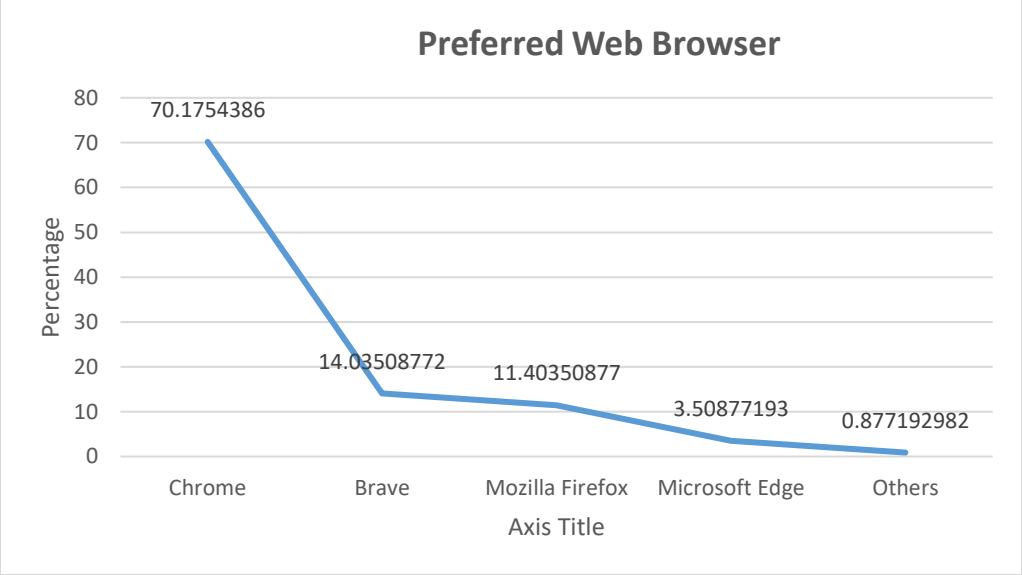


Figure 3 preferred web browser

4.1.4 Software Update Frequency:

A significant number of participants opt for regular software updates, with 75 respondents (monthly updates) and 18 respondents (weekly updates). This portrays a proactive approach to maintaining system security and functionality. However, a minority opting for daily or yearly

updates highlights varying levels of awareness and habits regarding software updates. It's crucial to encourage and educate individuals on the importance of timely software updates for enhanced security.

Software Update Frequency:		
Options	**Responses**	**Responses (in %)**
Daily	6	5.263157895
Weekly	18	15.78947368
Monthly	65	57.01754386
Yearly	25	21.92982456
Total	**114**	**100**

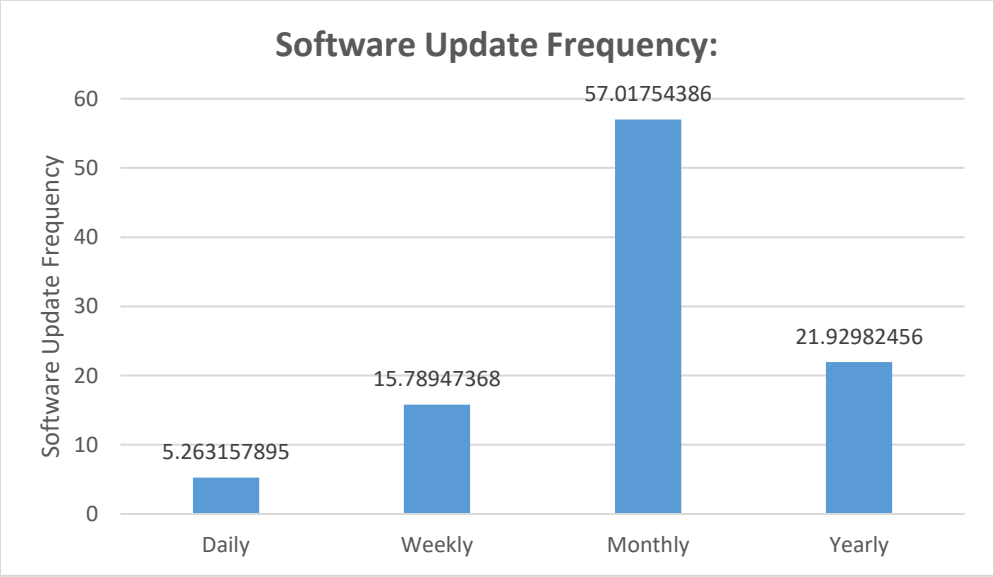


Figure 4 Software update frequency

4.1.5 Comfort Level with Sharing Personal Data

A notable portion (51 responses) express discomfort regarding sharing personal data for personalized services or targeted advertising. This signifies a cautious approach towards data sharing, prioritizing privacy over tailored experiences. Conversely, a smaller group (26 responses) feels comfortable or very comfortable, suggesting a more lenient approach to data sharing for enhanced service personalization.

4.1.6 Organization Communication on Data Privacy

The responses indicate a division in opinion regarding organizations' communication of data privacy and security practices. While 43 participants believe that organizations effectively communicate these practices, 40 respondents express skepticism. This division highlights the need for organizations to enhance transparency and communication to address the skepticism and build trust among individuals concerning data privacy.``````````````````

4.1.7 Safety of Sharing Personal Data Publicly

A significant majority (68 responses) believe that sharing personal data publicly is not safe. This reflects prevalent concerns regarding the potential risks associated with public data sharing, including privacy breaches and misuse. Conversely, a smaller group (15 responses) considers it safe, showcasing differing opinions and comfort levels regarding public data sharing.

Safety of Sharing Personal Data Publicly:		
Options	**Responses**	**Response (in %)**
Yes	30	26.31578947
No	84	73.68421053
Total	**114**	**100**

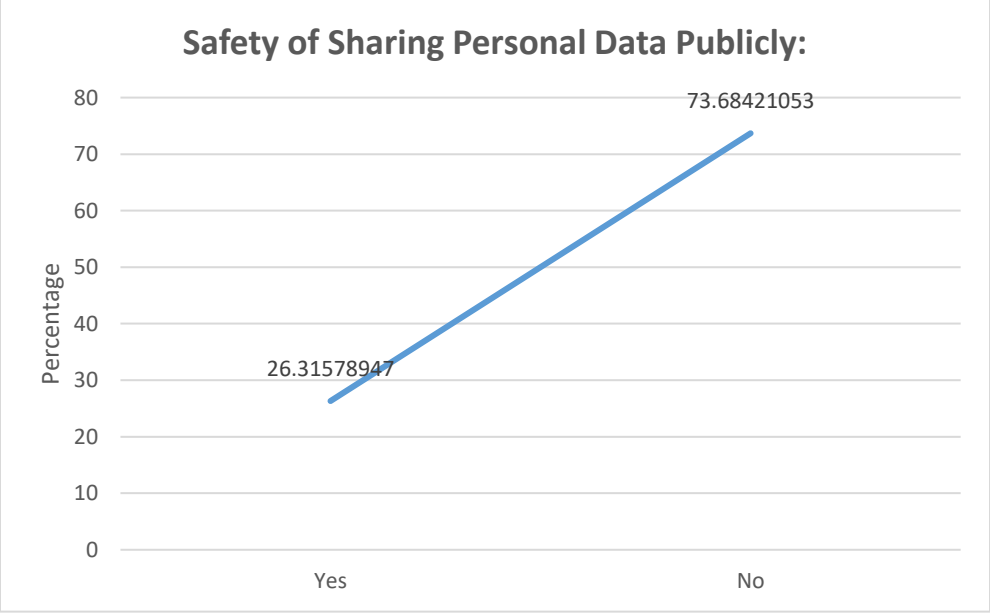


Figure 5 Safety of Sharing Personal Data Publicly

In conclusion, the analysis of these questions reveals a group of respondents who generally understand data privacy and prioritize caution when it comes to sharing personal information. There's a need for ongoing education, especially regarding the significance of regular software updates and promoting best practices for data protection. Additionally, enhancing transparency in organizational communication regarding data privacy practices is vital to address skepticism and build trust.

Chapter 5 Discussion, Conclusions and Implications

5.1 Discussion

In assessing awareness and behavior patterns related to data privacy and security our findings illuminate a multifaceted landscape. While there is a discernible uptick in awareness regarding the significance of data privacy and security, a substantial number of individuals still engage in risky behaviors. The study unveils several key observations:

Individuals predominantly rely on personal gadget devices like smartphones, tablets, and laptops, underscoring the necessity for enhanced security practices on these devices, given their central role in daily life. In terms of social media preferences, convenience and engagement often take precedence over privacy considerations, with participants frequently sharing personal information and interacting with third-party apps without fully acknowledging potential risks. Password security emerges as a notable concern, as a significant number of participants use weak passwords or engage in password reuse across multiple accounts, presenting a clear vulnerability to malicious exploitation. The study also reveals that many individuals store sensitive data in the cloud, raising questions about the security of these services, despite robust security measures implemented by cloud providers. Additionally, participants frequently engage in risky online behaviors, such as clicking on suspicious links and downloading files from untrusted sources, underscoring the imperative for improved digital literacy and heightened awareness of online threats.

Participants generally exhibit limited knowledge of data privacy laws and regulations within their respective countries. This knowledge gap likely contributes to their risky online behaviors, as they may not fully comprehend their rights and the protections in place. Notably, there exists a strong correlation between participants' knowledge of data privacy laws and their attitudes toward sharing personal data and trusting third-party entities. Those with a deeper understanding of the legal framework tend to exercise greater caution in sharing personal information and have heightened expectations of privacy protection.

5.2 Conclusions

My study sheds light on the intricate landscape of data privacy and security awareness and behavior patterns, as well as the knowledge and perceptions of data privacy laws and regulations. While there is a discernible increase in awareness regarding the importance of safeguarding personal data, many individuals still engage in risky online behaviors, such as weak password practices and careless data storage. This underscores the urgent need for comprehensive educational initiatives, targeting safe gadget device usage, password security, and heightened digital literacy. Moreover, our findings underscore the pivotal role of legal frameworks in shaping individuals' attitudes and behaviors. Strengthening and simplifying data privacy regulations can instill a culture of privacy and security. Achieving a balance between convenience and privacy in the digital age is paramount, empowering individuals to make informed decisions about their data. As we move forward, it is imperative for policymakers, educators, and businesses to work collaboratively, promoting responsible data practices, technological advancements, and corporate responsibility to foster a more secure and privacy-conscious digital ecosystem for individuals and society as a whole.

5.3 Implications

Now, let's talk about what all these findings, In light of our study's findings, several significant implications emerge. Firstly, policymakers should consider the enhancement and simplification of data privacy regulations to make them more accessible to the general public. These regulations should evolve in tandem with the dynamic digital landscape to ensure comprehensive protection of individuals' rights while motivating businesses to adopt robust data security measures in compliance. Moreover, educational and awareness initiatives must be prioritized by public and private organizations. Targeting diverse demographics, these programs should emphasize responsible data management, online safety, and the potential consequences of risky digital behaviors. Technological innovation plays a vital role, with tech companies urged to improve default privacy settings on devices and applications, enabling users to customize their preferences intuitively. Companies entrusted with personal data should embrace corporate responsibility, implementing stringent data protection measures, transparent privacy policies, and clear communication of their commitment to data security to cultivate and maintain trust with customers. Collaboration among governments, educational institutions, businesses, and advocacy

groups is imperative to develop a holistic approach to data privacy and security, fostering the sharing of best practices and resources. Research and development efforts should be sustained to address emerging threats, while global cooperation should be encouraged to harmonize data protection standards across borders. In summary, our study underscores the pivotal roles of education, legal frameworks, and individual responsibility in nurturing a culture of data privacy and security, advocating for a balanced approach that ensures convenience while safeguarding the digital landscape for individuals and society as a whole.

References

Yaqi Gong Dr. Ashley Schroeder A systematic literature review of data privacy and security research on smart tourism

https://www.sciencedirect.com/science/article/abs/pii/S2211973622000848

Privacy Prevention of Big Data Applications:

https://journals.sagepub.com/doi/full/10.1177/21582440221096445

Personal Data Online and Data Privacy:

https://ukdiss.com/litreview/personal-data-privacy-solution-3424.php

Data Privacy Issues and Challenges:

https://www.juw.edu.pk/resource/uploads/2021/04/3.-Compter-Science-Renu-Bala.pdf

Data Security in Cloud Computing:

https://www.ijert.org/a-review-on-data-security-in-cloud-computing

Appendices

Appendix: Form Questions

1. Your FullName
2. Gender
    a) Male
    b) Female

3. Your Age?

4. What are the devices you use?
    a) Phone
    b) Laptop
    c) Tablet
    d) Desktops
    e) Others
5. Do you use mobile, which one you use?
    a) Facebook
    b) Instagram
    c) Twiter
    d) linkedIn
    e) tiktok
    f) Youtube
    g) others

6. Do you use secure password?
    a) Yes
    b) No

7. Where do you store your important files?
    a) Google drives
    b) Pen drives/hard drives
    c) Phone
    d) Others

8. Which web browser do you normally use?
    a) Chrome
    b) Brave
    c) Mozilla Firefox
    d) Microsoft Edge
    e) others
9. How often do you use Update for software?
    a) Daily
    b) Weekly
    c) Monthly
    d) Yearly
    e) Others

10. Do you have anti-virus software installed on your computer?
    a) Yes
    b) No
11. Do you trust companies and institutions that they will not misuse your data?
    a) Yes
    b) No

12. How often do you backup your important data to protect it from loss?
    a) Weekly
    b) Monthly
    c) Yearly
    d) Others

13. Are you concerned about the privacy and security of your personal data?
    a) Yes
    b) No

14. Do you use two factor authentication for your account?
    a) Yes
    b) No
15. Have you ever experienced a privacy or security breach related to your personal data?
    a) Yes
    b) No
16. Are you aware of the types of personal data that organizations collect about you?
    a) Yes
    b) No
17. How comfortable are you with sharing personal data in exchange for personalized services or targeted advertising/advertisement?
    a) Comfortable
    b) Uncomfortable
    c) Neutral

18. Do you believe that organizations should obtain consent from individuals before collecting or using their personal data?
    a) Yes
    b) No

19. Are you aware of the data privacy laws and regulations in our country?
    a) Yes
    b) No

20. Do you think organizations communicate their data privacy and security practices to the public?
    a) Yes
    b) No

21. Do you think there should be strict rule and regulation to protect personal data?
    a) Yes
    b) No
22. Do you check the link that you get from other is harmful or safe?
    a) Yes
    b) No
23. Do you use public WIFI ?
    a) Yes
    b) No
24. How often do you review and manage the permissions granted by your device?
    a) Daily
    b) Weekly
    c) Monthly
    d) Yearly
    e) Others

25. Have you ever encountered phishing attempts or fraudulent emails?
    a) Yes
    b) No
26. Have you ever used a VPN (virtual private network)?
    a) Yes
    b) No
27. Have you shared your ID password of any social media to other?
    a) Yes
    b) No
28. Any Suggestion regarding questions and this project?

THANK YOU