

CYBER SECURITY AWARENESS FOR PARENTS AND WOMEN PERSPECTIVE

BY

**ADIBA ZAMAN CHOWDHURY
ID: 203-15-3924
AND**

**FARHAN ADNAN
ID: 203-15-3919**

FINAL YEAR DESIGN PROJECT REPORT

This Report Presented in Partial Fulfillment of the Requirements for the
Degree of Bachelor of Science in Computer Science and Engineering

Supervised By

Mr. Amit Chakraborty Chhoton
Assistant Professor
Department of CSE
Daffodil International University

Co-Supervised By

Afjal Hossain Sarower
Lecturer (Sr. Scale)
Department of CSE
Daffodil International University



DAFFODIL INTERNATIONAL UNIVERSITY

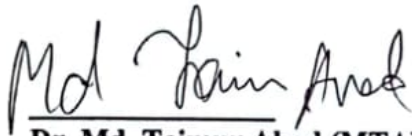
DHAKA, BANGLADESH

July 2024

APPROVAL

This Project titled “Cyber Security Awareness for Parents and Women Perspective”, submitted by **Adiba zaman chowdhury** and **Farhan Adnan** to the Department of Computer Science and Engineering, Daffodil International University, has been accepted as satisfactory for the partial fulfillment of the requirements for the degree of B.Sc. in Computer Science and Engineering and approved as to its style and contents. The presentation has been held on 13-07-2024.

BOARD OF EXAMINERS



Dr. Md. Taimur Ahad (MTA)
Associate Professor & Associate Head
Department of CSE
Faculty of Science & Information Technology
Daffodil International University

Board Chairman



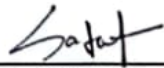
Dr. Fizar Ahmed (FZA)
Associate Professor
Department of CSE
Faculty of Science & Information Technology
Daffodil International University

Internal Examiner 1



Mr. Rahmatul Kabir Rasel Sarker (RKR)
Lecturer
Department of CSE
Faculty of Science & Information Technology
Daffodil International University

Internal Examiner 2



Sadat Hasan
Data Scientist (Senior Principal Officer)
Risk Management Division
BRAC Bank

External Examiner

DECLARATION

We hereby declare that this project has been done by us under the supervision of **Mr. Amit Chakraborty Chhoton**, Assistant Professor, Department of Computer Science and Engineering, Daffodil International University. We also declare that neither this project nor any part of this project has been submitted elsewhere for the award of any degree or diploma.

Supervised by:



Mr. Amit Chakraborty Chhoton
Assistant Professor
Department of CSE
Daffodil International University

Co-Supervised by:

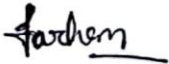


Afjal Hossain Sarower
Lecturer (Sr. Scale)
Department of CSE
Daffodil International University

Submitted by:



Adiba zaman chowdhury
ID: 203-15-3924
Department of CSE
Daffodil International University



Farhan Adnan
ID: 203-15-3919
Department of CSE
Daffodil International University

ACKNOWLEDGEMENT

First, we express our heartiest thanks and gratefulness to almighty for His divine blessing making it possible for us to complete the final year project/internship successfully.

We are grateful and wish our profound indebtedness to **Mr. Amit Chakraborty Chhoton, Assistant Professor**, Department of CSE Daffodil International University, Dhaka. Deep Knowledge & keen interest of our supervisor in the field of “*Cyber Security Awareness*” to carry out this project. His endless patience, scholarly guidance, continual encouragement, constant and energetic supervision, constructive criticism, valuable advice, reading many inferior drafts, and correcting them at all stages have made it possible to complete this project.

We would like to express our heartiest gratitude to the **Head of the Department of CSE**, for his kind help in finishing our project and also to other faculty members and the staff of the Department of CSE, Daffodil International University.

We would like to thank our entire course mate in Daffodil International University, who took part in this discussion while completing the course work.

Finally, we must acknowledge with due respect the constant support and patience of our parents.

ABSTRACT

This abstract outlines a comprehensive approach to fostering cybersecurity awareness tailored specifically for parents' and women' in Bangladesh. With the escalating prevalence of cyber threats in the digital age, it has become imperative to prioritize cybersecurity awareness among diverse demographics, including parents and women. It discusses the importance of understanding online threats, safety measures, and the role of education in promoting a digital environment. Therefore, our study aims to investigate the extent to which parents and women are aware of cybersecurity. A sample of 698 parents, including 410 males and 296 females, was targeted through an online questionnaire. From the data gathered, it was found that parents have a good understanding of cyber threats and are committed to safeguarding their family members from such dangers. However, this knowledge needs to be translated into action by both parents and authorities through concrete steps.

Keywords:

Cybersecurity; Awareness; cyber threats; Bangladesh.

TABLE OF CONTENTS

Contents	Page No
Board of Examiners	i
Declaration	ii
Acknowledgments	iii
Abstract	iv
 CHAPTER 1: INTRODUCTION	 1-11
1.1 Overview	1-2
1.2 Background and Present State	2
1.3 Problem Statement	3
1.4 Objectives	4-7
1.5 Scope and Limitations	7-9
1.6 Report Organization	9-11
1.7 Summary	11
 CHAPTER 2: LITERATURE REVIEW	 12-18
2.1 Overview	12-13
2.2 Related Works	13-15
2.3 Comparison between existing works	15-17
2.4 Open Issues	17-18
2.5 Summary	18
 CHAPTER 3: METHODOLOGY/ REQUIREMENT ANALYSIS & DESIGN SPECIFICATION	 19-37
3.1 Overview	19
3.2 Proposed Methodology/ System Design	19-31
3.3 Hardware/ Software Requirement	32-33

3.4 Project Management and Financial Analysis	33-36
3.5 Summary	36-37
CHAPTER 4: IMPLEMENTATION	38-45
4.1 Overview	38
4.2 Train Model/ Prototype Design	39-41
4.3 System Testing/ Model Evaluation	42-45
4.4 Summary	45
CHAPTER 5: RESULT AND ANALYSIS	46-65
5.1 Overview	46
5.2 Experimental/ Simulation Result	46-54
5.3 Performance/ Comparative Analysis	54-64
5.4 Summary	64-65
CHAPTER 6: IMPACT ON SOCIETY, ENVIRONMENT AND SUSTAINABILITY	66-74
6.1 Impact on Life	66-67
6.2 Impact on Society & Environment	68-69
6.3 Ethical Aspects	69-71
6.4 Sustainability Plan	71-73
6.5 Summary	73-74
CHAPTER 7: CONCLUSION AND FUTURE WORK	75-80
7.1 Conclusions	75-77
7.2 Further Suggested Works	77-78
7.3 Limitations/ Conflict of Interests	78-80

REFERENCES	81
APPENDIX A	82-87
APPENDIX B	

LIST OF FIGURES

Figures	Page no
Figure 3.2.0: Agile Methodology	19
Figure:3.2.1: Methodology of the paper	20
Figure 3.2.2: Website Decision flowchart	21
Figure 3.2.3: Website Flow chart for students	22
Figure 3.2.4: Website Flow chart for Admin	22
Figure 3.2.5: Website Use case Diagram	23
Figure 3.2.6: Website ER Diagram	23
Figure 3.2.5: Website Home page	24
Figure 3.2.6: Website Home page	24
Figure3.2.7: Website Service	25
Figure 3.2.8: Awareness course	25
Figure 3.2.9: A video About cybersurokkha	26
Figure 3.2.10: Blog post section	26
Figure 3.2.11: login page from students	27
Figure 3.2.12: login page from Admin	27
Figure 3.2.13: know About us	28
Figure 3.2.14: Single course details page	28
Figure 3.2.15: Single blog page	29
Figure 3.2.16: For upload the course	29
Figure 3.2.17: For saw all the uploaded course	30
Figure 3.2.18: For uploaded blog	30
Figure 3.2.20: search box	31
Figure 3.3.1: MVC Architecture	33
Figure: 4.2.1 Prototype design home page	39
Figure: 4.2.2 Prototype design of login and signup page	39
Figure: 4.2.3 After login homepage prototype design	40
Figure: 4.2.4 Blog page prototype design	40

Figure: 4.2.5 Course page prototype	41
Figure: 4.2.6 Course details page prototype	41
Figure: 4.3.1 Shows the chatbot input data	42
Figure: 4.3.2 Course input Data	42
Figure: 4.3.3 Admin input Data	42
Figure: 4.3.4 User Data Input	43
Figure: 4.3.5 Message store Database	43
Figure 4.3.6: chatbot data store table	44
Figure 4.3.7: Delete course from database	45
Figure 5.2.0: Cyber security awareness is important or not	62

LIST OF TABLES

Tables	Page no
TABLE 2.3.1: Comparative Analysis Table	16
TABLE 3.4.1: Estimated Cost for Web Development Project	36
TABLE 4.2.1: Childs' Awareness Table	52
TABLE 5.2.2: Parents' Awareness Table	55
TABLE 5.2.3: Parents' Awareness Summary Table	58
TABLE 5.2.4: Womens Awareness Table	60

CHAPTER 1

INTRODUCTION

1.1 Overview

This has changed the way we live, work and communicate due to introduction of Digital age. But this technological advancement has also resulted in a rapid rise of cyber attacks causing major issues both individuals and families. This study offers a detailed insight into the current landscape of cyber security awareness, taking particular interest in parental and female perspectives.

During this process, the paper is structured into some significant chapters that discuss various important facets of cybersecurity from different standpoints. The first section establishes the context by providing a wider perspective on emergent digital threats that penetrate our daily lives. In fact, it speaks about the dynamic nature of cyber risks and continuous adjustments to new threats.

After this, the paper goes into detail about parents' unique function in protecting their children internet lives. To equip parents' capabilities of the necessary knowledge in order to create a relatively secure online presence for their offspring by exploring some common cyber threats families face, such as internet predators, cyberbullying etc.

The next section will be dedicated to women-specific challenges in the virtual field. It covers topics like cyber bullying, digital identity theft and a form of technology-related gender violence. Through the identification and analysis of these challenges, we aim to provide our part for the creation of solutions strengthening cybersecurity consciousness among women in different aspects.

As the paper proceeds, it applies existing cybersecurity practices and pinpoints gaps in awareness and education. Through critical evaluations of the effectiveness of existing interventions, we intend to offer suggestions for improving initiatives directed towards specific target groups comprising parents and women with a proactive online safety perspective.

The study next discusses technology, which shapes the perceptions and behaviors pertaining to cybersecurity. So, we are able to design appropriate awareness campaigns and interventions based on our understanding of the dynamics through which technological innovations affect people's interactions with their digital environment.

It is in the final section; however, this paper integrates prominent results and provides a plan for building up resilient digital community. We hope to help in creating a more educated society that will be able to better navigate through the digital world safely and make informed decisions ant cyber threat scenarios. By exploring all these aspects, we are ultimately trying to fill the gap in cybersecurity awareness and finding a way for people as well as families safe on Internet.

1.2 Background & Present State

Background

The purpose of this study is to understand the underlying motivation that led me to carry out a research in order to cope with the growing threats emanating from cyber during our age characterized as information everyday. Given the extent to which our lives are increasingly tied up with digital boarders, parental and female weaknesses deserve more credence. However, the current gaps in cybersecurity awareness that are carefully designed for these demographic groups reflect a critical need to conduct an encompassing case study. In doing so, this study hopes to advance the creation of unique strategies aimed at uplifting individuals with regard their ability and confidence in negotiating an online domain that is ridden by complex issues – such as those faced by parents or women. The broad aim is to promote a safer and more secure online environment that meets the varying necessities of these key pillars.

Present state

Our website is now almost prepared. We are working on course videos and blogs about cyber threats. We will have online free courses about the ongoing cyber threats so that anyone can visit our website and do the course for their knowledge and stay safe.

1.3 Problem Statement

In modern times, the applications of technology have never been as excessive and challenging than they are now. This is based on a growing incidence and complexity level of cyber threat to people in families' life. The challenge is more prevalent for technicians who include parents and women whose views in the world of cybersecurity require special analysis. With the evolution of a more interconnected digital environment, it becomes apparent that most awareness campaigns fail to speak directly about concerns related to these groups in our society.

- **Unaware of Cyber threats :** It's seen that parents and women of our society is mostly unaware of the cyber threats . They don't know about the ongoing cyber crimes and how they are affecting people. That's why most of the time they fell for the cyber traps.
- **Lack of knowledge :** In most of time we have seen that in some cases if the targeted people knows about the threats they don't know how to overcome the threats. For this reason when they fell for the cyber traps they couldn't find any kind of solution to overcome the situation.
- **Limited resources :** In our country we don't have a specific platform that works with this kind of threats. That's why it's become so difficult to make people aware about the threats and situations. Many campaigns are being held on that topic but they just can't go to somewhere and find the solution.
- **Awareness guide :** In so many journals and campaigns people tried to make people educated and aware about the basics of cyber security. But there is no specific platform for that. So, through our platform they will know be able to learn the basics and will be able to become aware.
- **Accessibility :** As by the time the platform grows, we will have a big user base. It will be hard to maintain it's accessibility .

1.4 Objectives

The purpose of this study is to understand the underlying motivation that led me to carry out a research in order to cope with the growing threats emanating from cyber during our age characterized as information everyday. Given the extent to which our lives are increasingly tied up with digital boarders, parental and female weaknesses deserve more credence. However, the current gaps in cybersecurity awareness that are carefully designed for these demographic groups reflect a critical need to conduct an encompassing case study. In doing so, this study hopes to advance the creation of unique strategies aimed at uplifting individuals with regard their ability and confidence in negotiating an online domain that is ridden by complex issues – such as those faced by parents or women. The broad aim is to promote a safer and more secure online environment that meets the varying necessities of these key pillars. They are listed below :

Investigate the cyber threats posed to parents and women, I.E online predators, cyber-bullying, identity theft among other forms of gender based violence in cyberspace.

Assess the harm brought to families and individuals by these perils in order to gain a deeper experience of challenges presented.

Evaluate how well the traditional awareness programs address parents' and women specific concerns. Find gaps and deficiencies in current educational resources and method, with emphasis on distinguishing projects toward these populations.

Propose Tailored Educational Strategies:

Create customized cybersecurity awareness programs that provide parents with the information and training required to effectively secure their households from threats.

Develop approaches that address the unique cyber security threats targeting women, thereby fostering an ideology of initiative in matters digital safety.

Conduct an analysis of the effect that technological developments have on parental perceptions and her/his behavior related to cybersecurity.

Know how emerging technologies affect digital exchanges and create sensitization campaigns consistent with new trends in the development of technology.

Comment on policy considerations that can help to strengthen cybersecurity awareness for parents and women promoting a comprehensive approach.

Partner with the stakeholders involving various governmental bodies and educational establishments to create policies that ensure digital security is reinforced.

Analyze study results into practical recommendations as solutions guiding various individuals, families and communities to maneuver through the online world while being safe.

Develop an environment that promotes vigilance and preparedness, thus helping to establish a better-informed cyberspace.

This study aims at filling the existing gaps in cybersecurity awareness to make available tangible solutions resonating with parents and women online. This is what we try to achieve by undertaking these efforts in order to enable a paradigm shift towards a more sustainable and resilient digital ecosystem.

This study encompasses cybersecurity awareness comprehensive studying parents and women perception from digital era. The project will analyze the specific hurdles that these groups encounter in their new environment, with a focus on providing viewpoints and solutions to benefit them while enjoying digital technology.

1.4.1 Demographic Focus:

Parents: Analyze the cybersecurity threats parents grapple with when safeguarding their children's digital lives. This entails problems like online predators, cyberbullying and seeing content that is inappropriate.

Women: Research the unique cybersecurity issues faced by women that appears in online harassment, identity theft and the relationship between technology with gender-based violence.

1.4.2 Cyber Threat Analysis:

Identify and critically evaluate surging cyber dangers in relation to parenting as well the vulnerable of families, regarding women embedded towards changeable culture.

Investigate how such perils affect the welfare of families and individuals, stressing the necessity to run focused initiatives in this regard.

Evaluate the performance of already existing cybersecurity awareness campaigns to meet the needs and concerns of parents as well women.

Detect the blanks and weaknesses of the current educational resources and methods, where different initiatives are to be adjusted according to these demographic segments

Establish cybersecurity awareness programs that are user-specific and designed to equip parents with the appropriate knowledge as well as skills aimed at creating secure online environment for their families.

Suggest measures that consider the unique issues in cyber security for women, leading to a more comprehensive and preventative approach towards digital safety.

1.4.3 Exploration of Technology's Influence:

Research the effect of technology driven developments on mindsets and actions concerning cybersecurity among parents, as well women.

Understand digital interactions and how emerging technologies change them; this should lead to improved awareness campaigns based on modern trends in the sphere of digitization.

1.4.4 Policy Considerations:

Outline policy considerations that will improve cybersecurity awareness on the part of parents and women, championing for a broad based approach.

Partnerships with stakeholders, such as government agencies and academic institutions

need to ensure the creation of policies that improve digital safety.

Summarize findings from various studies as actionable recommendations for individual, family and society level practices that assist in proceeding the virtual world safely.

Encourage culture of vigilance & preparedness, leading to a better and more vibrant digital nation.

The study will utilize both qualitative and quantitative methodologies that involve surveys, interviews, data analysis, and other techniques for insight generation. The spatial breadth may be comprised of many regions to ensure a broad-based perspective on the difficulties faced by parents and women residing in different cultural environments characterized with specific socioeconomic conditions. The findings and recommendations of the study seek to address what are currently perceived as gaps in cybersecurity awareness, thereby providing practical solutions for a safer community marked by resilience against threats from cyberspace.

1.5 Scope & Limitations

The study delivers a thorough examination of its results, highlighting notable differences in cyber education and parental engagement, as well as their substantial impacts on children's embrace of online safety measures. It emphasizes essential observations into areas requiring enhancement, emphasizing the crucial importance of strong cyber safety training and proactive parental support. The results stress the importance of unified endeavors to boost children's digital skills and guarantee their safe exploration of the online realm.

The conclusion of this study can be viewed as a multilateral contribution answering the problem to enrich cybersecurity awareness for women and parents, especially in terms of creating more secure communities online. The aim of this project is to create products that are realistic and practical in empowering people, the family unit, or community as a whole with confidence into digital space.

1.5.1 Insights into Unique Cybersecurity Challenges:

A well-rounded overview of unique cyber security threats posing to parents and women, backed up by detailed descriptions of predominant menaces as those that influence people in families or individuals.

Critique of current cybersecurity awareness programs, comparing whether they sufficiently addresses the issues raised by parents and women based on some observations covering what currently exists in terms of any gaps and opportunities for further enhancements.

1.5.2 Tailored Educational Strategies:

Design sophisticated and personalized cyber security awareness programs that could provide parents with the knowledge and skills necessary for building a safe internet ecosystem within their families.

Strategies development oriented approach to specific cyber safety needs of women, high proactive attitude to digital security.

1.5.3 Understanding Technology's Impact:

Understanding the impact technological improvements have on parental and women's perceptions behavior concerning cybersecurity that can help in understanding which awareness campaign will work best with changing digital cultures.

1.5.4 Policy Recommendations:

Proposed policy considerations to increase the level of cybersecurity awareness among parents and women should include taking a holistic approach by involving government organizations and learning institutions.

1.5.5 Community Empowerment:

The findings of synthesized research were presented through an action-oriented conclusions that could guide individuals, families and communities to securely navigate

the digital terrain.

Creating an enlightened and alert culture or attitude that will lead to the development of a safer and well-informed digital society.

1.5.6 Dissemination of Knowledge:

Publications of research results in academic journals, conferences and also in format readable by wide audience such as policy makers, educators or the general public.

Provision of educational materials and resources off shooting the research to catalyze widespread dispersion of cybersecurity know how.

1.5.7 Long-term Impact Assessment:

Setting up measures for regular evaluation to assess the duration impact of research results on parent awareness and practice in women about cybersecurity.

Iterative feedback loops to improve and perfect educational approaches in accordance with contemporary digital dangers, as well as the rate of technological progress.

Therefore, by attaining these results as a consequence the research seeks to support in establishing resilient and safe digital community where (parents/ women) will be empowered with all capabilities they need for navigation of their virtual territories without stakes and threats on themselves or families.

1.6 Report Organization

The proposed report has a well-structured layout designed to help readers navigate through the research process, findings, and implications. Each chapter serves a specific purpose, enhancing the overall coherence and depth of the document.

Chapter 1: Introduction

The introductory chapter establishes the context for the research by detailing the importance of cybersecurity awareness for parents and women. It outlines the study's

objectives and the overall framework of the project.

Chapter 2: Literature Review

This chapter delves into relevant literature and previous research, providing a comprehensive understanding of theoretical foundations, methodologies, and technological advancements related to cybersecurity awareness. It also identifies gaps in current knowledge and sets the stage for the present study.

Chapter 3: METHODOLOGY/ REQUIREMENT ANALYSIS & DESIGN SPECIFICATION

The methodology chapter outlines how the study was conducted, including research design, data collection methods, analysis techniques, and rationale for selecting specific methodologies. Ethical considerations and potential study limitations are also addressed.

Chapter 4: Experimentation

In this chapter, the experimental results obtained from the study are presented. Detailed analyses of findings are included, along with visual representations and statistical measures to support the outcomes.

Chapter 5: Results and Analysis

This project increases cybersecurity awareness among parents and women through information gathering and education. Google Forms surveys collect data on cybersecurity practices, which are analyzed in Google Collab to identify key concepts. The data informs the development of the website through the use of HTML, CSS, JavaScript, and PHP, including contact forms and graphics for sharing insights. The website integrates ethical standards to ensure confidentiality and informed consent.

Chapter 6: IMPACT ON SOCIETY, ENVIRONMENT AND SUSTAINABILITY

Officers of this organization will call approximately 2000 parents without their children's knowledge and explain to them the key concepts of cybersecurity through the CyberSurokkha platform created for these purposes. It emphasises the concept of locating existing knowledge gaps and respondents and offering educational resources in the form

of friendly courses and a blog. Its implementation propels ideal forms of learning that involve interactivity and support from members of the society with an emphasis on practicing safe use of the internet within homes and neighborhoods.

Chapter 7: CONCLUSION AND FUTURE WORK

This chapter shows the summary of the whole paper and what future works can be possibly done with this project and how we can make people beneficial through our website.

1.7 Summary

This report covers the lacking of others works based on Cyber security awareness. We have studied many reports and analysis to find out the problems that our targeted audience is facing and how to solve the issue. We offer free courses to aware people. We have done comparison between related works and Gap analysis to make a platform which will be able to make our target audience easy to face cyber threats and cyber related frauds. Methodology shows how our platform works and what we are doing. How our Simple work can make a big change to save many issues is our goal .

CHAPTER 2

LITERATURE REVIEW

2.1 Overview

The landscape of cybersecurity awareness among parents and women involves a wide array of activities designed to empower individuals in safely navigating the digital realm. These encompass online safety guides, awareness campaigns, research studies, workshops, training programs, forums, advocacy efforts, partnerships, and corporate initiatives. By engaging with these endeavors, stakeholders can access valuable resources and opportunities to boost cybersecurity awareness for parents and women. Collaboration across different sectors is crucial for addressing cyber threats and fostering a secure online environment for everyone. numerous papers have been reviewed to highlight the challenges faced by our target audience and the extent to which they are susceptible to cyber threats. Our project aims to not only identify these issues but also educate them on the fundamentals of cybersecurity and online dangers.

Cybersecurity: Cybersecurity involves protecting systems, networks, and programs from digital attacks. These cyberattacks aim to access, alter, or destroy sensitive information, extort money, or disrupt normal business operations.

Cybercrime: Cybercrime refers to criminal activities conducted using computers or the internet. Typical cybercrimes include identity theft, phishing, and hacking.

Phishing: Phishing is a social engineering attack used to steal user data like login details and credit card numbers. This occurs when an attacker pretends to be a trusted source to trick a victim into opening an email, message, or text.

Ransomware: Ransomware is malicious software that blocks access to a computer system until a ransom is paid. It spreads through phishing emails or exploiting software vulnerabilities.

Malware: Malware is malicious software intended to harm computers, servers, clients, or networks. The term combines "malicious" and "software."

Cyber Hygiene: Cyber Hygiene refers to practices users follow to maintain system health and enhance online security. Good cyber hygiene includes using strong passwords, updating software, and being careful with email attachments.

Encryption: Encryption is the process of converting data into code to prevent unauthorized access.

Firewall: A Firewall is a network security system controlling incoming and outgoing traffic based on security rules. It acts as a barrier between trusted and untrusted networks.

2.2 Related Works

Recently, the increasing importance of cybersecurity has highlighted its crucial role in protecting parents and women online. In a study by N. Ahmad@Ahmad Arifin and colleagues, the focus is on "Parental Awareness on Cyber Threats Using Social Media." The findings suggest that Malaysian parents possess a moderate level of awareness regarding cyber threats through social media. This underscores essential need for enhancing early exposure to cybersecurity education[1].

In a recent article by Hussein, O.A. (2022) titled "Cyber Blackmail Crime Against Women- A Case Study," the discussion revolves around cyber blackmail targeting women in Iraq. The article sheds light on the prevalence, challenges, and reasons behind the expansion of this criminal activity. It further delves into the analysis of legislation, community awareness, litigation processes, and prevention strategies for involved stakeholders[2].

J.Babu and P. Jayakumar conducted a study in 2020 on the "Attitude and Awareness of Women about Cyber Sexual Offences." The research reveals that women in India showcase a positive attitude towards cyber sexual offenses. However, there is a lack of awareness concerning IT Act services among them, rendering them more susceptible to falling victim to cybercrimes[3].

A recent publication by A.A. Alghamdi (2022) entitled "Parents' Awareness of Cybersecurity" from Majmaah University's Publishing and Translation Center explores the Journal of Engineering and Applied Sciences. The journal serves as a platform for advanced research in various engineering domains, presenting an extensive editorial board comprising experts in their respective fields[4].

Verma, D.K., Verma, V., Pal A., and Verma D. (2022) highlight issues surrounding the "Identification and mitigation of cyber crimes against women in India." The discussion encompasses various cyber crimes targeting women such as privacy invasion, online grooming, bullying, and harassment. It underscores the rising complexity of these crimes alongside the inadequate computer and internet literacy among female individuals[5].

P.R.D.M Suriakala focuses on "AN ANALYTICAL STUDY ON CYBER STALKING AWARENESS AMONG WOMEN USING DATA MINING TECHNIQUES." This research delves into the realm of cyber stalking awareness among women in Chennai, India using innovative data mining techniques. It draws attention to the prevalence of cyber stalking among emotionally vulnerable women while proposing protective measures for averting such occurrences[6].

In Mostovaia's (2020) qualitative examination on parents' awareness of online predatory behaviors uncovers critical insights into familiar online spaces accommodating predatory activities along with trends and statistics related to child sexual abuse online. The discourse extends to online advantages, hazards, alarming behaviors exhibited online, as well as strategies aimed at safeguarding children from potential harm inflicted by online sexual predators[7].

The study conducted by THAKUR, D.S., addresses "Cyber Crimes and Victimization of Women in India with Special Reference to Cyber Obscenity." This comprehensive discourse traverses through various cyber crimes targeting women in India including harassment, stalking pornography defamation and morphing incidents highlighting gender bias prevalent within these crimes while also addressing issues surrounding authority deficits observed within this domain. The escalating incidents of cybercrime against women can be attributed to an upsurge in internet users coupled with the anonymity afforded by digital platforms[8].

A study conducted by Chahak Mittal in (2024) delved into cybersecurity awareness and concern levels in Punjab, India. The findings highlighted that young adult females aged 18 to 29 are exceptionally susceptible to cyber threats. The study underscored the necessity for targeted measures to enhance cybersecurity defenses for this specific group[9].

Research carried out by Shah in (2019) analyzed the nature and scope of cybercrimes in India. It brought attention to the escalating reliance on the internet and the subsequent increase in cyber vulnerabilities. The research pointed out that a significant number of cybercrimes revolve around financial fraud, data theft, and online harassment, with women and children being primary targets[10].

A thorough examination by Kumar and Manhas in (2021) regarding cybercrimes in India outlined various patterns and precautionary steps. The study recognized the difficulty in tracking down cybercriminals due to the internet's global nature and emphasized the

significance of cybersecurity education and strong legal frameworks to tackle cyber threats [11].

2.3 Comparative Analysis and Summary

In comparing cybersecurity awareness and practices across various regions, distinct differences and similarities become apparent.

When it comes to Awareness Levels, research shows that cybersecurity awareness varies significantly among different demographics and regions. Young adults residing in urban areas typically exhibit higher levels of awareness than those in rural regions. Gender also plays a role, with women generally receiving less exposure to cybersecurity training compared to men.

Regarding Cybercrime Types, the prevalent cybercrimes differ from one region to another. While financial fraud and data theft are widespread globally, regions like South Asia observe more cases of online harassment and cyberbullying, especially targeting women and children.

As for Preventive Measures, effective cybersecurity practices such as using strong passwords, keeping software updated regularly, and exercising caution online are universally recommended. However, the consistency in implementing these practices often falters, particularly in developing regions due to limited resources and education available.

TABLE 2.3.1: Comparative Analysis Table

SL No	Author Name	Used Algorithm	Best Accuracy with Algorithm
1	Ahmad et al. (2019)	Not specified	N/A
2	Hussein (2022)	Case Study	N/A
3	Babu & Jayakumar (2020)	Survey Analysis	N/A
4	Alghamdi (2022)	Survey Analysis	N/A
5	Verma et al. (2022)	Case Study	N/A
6	Suriakala	Data Mining Techniques	N/A
7	Mostovaia (2020)	Qualitative Analysis	N/A
8	Thakur	Not specified	N/A
9	Chahak Mittal (2024)	Survey Analysis	N/A
10	Shah (2019)	Survey Analysis	N/A
11	Kumar and Manhas (2021)	Survey Analysis	N/A

2.4 Open Issues

The scope of the problem addressed in this research, focusing on " Cyber Security Awareness for Parents and Women Perspective " In comparing cybersecurity awareness and practices across various regions, distinct differences and similarities become apparent.

When it comes to Awareness Levels, research shows that cybersecurity awareness varies significantly among different demographics and regions. Young adults residing in urban areas typically exhibit higher levels of awareness than those in rural regions. Gender also plays a role, with generally receiving less exposure to cybersecurity training compared to men.

Regarding Cybercrime Types, the prevalent cybercrimes differ from one region to another. While financial fraud and data theft are widespread globally, regions like South Asia observe more cases of online harassment and cyberbullying, especially targeting women and children.

As for Preventive Measures, effective cybersecurity practices such as using strong passwords, keeping software updated regularly, and exercising caution online are universally recommended. However, the consistency in implementing these practices often falters, particularly in developing regions due to limited resources and education available.

2.5 Summary

With this approach, the project develops the areas of parents and women's cybersecurity by providing online safety guides, awareness campaigns, research studies, workshops, training programs, forums, advocacy, partnerships, and a range of corporate activities. They are designed to educate people about lot of risks of the modern world Web and equip them with the tools to deal with danger.

Key Concepts

Cybersecurity: To shield systems, networks, and programs from an attack by hackers or unauthorized people.

Cybercrime: Cybercrime, fraud, which involves embezzlement of other people's identities

and proceeds frauds accomplished through the use of computers or the internet.

Phishing: Phishing and pretexting in order to steal a user's information under the guise of being someone that the user trusts.

Ransomware: Virus that prevents the users from utilizing the computer system and demands a certain amount of money to be paid in order to restore access.

Malware: Programs that are created purposely to infect computers, servers, clients and networks.

Cyber Hygiene: Measures that can be used to monitor the system and increase security on the internet.

Encryption: Almost acts of converting the data into the code to avoid having it accessed by unauthorized individuals.

Firewall: Traffic filter that regulates the incoming and outgoing connection according to the provided security protocols.

CHAPTER 3

METHODOLOGY/ REQUIREMENT ANALYSIS & DESIGN SPECIFICATION

3.1 Overview

Our goal is to build an effective web-based platform in order to raise awareness of cybersecurity concerns among Bangladeshi women and parents. This platform will use HTML, CSS, and JavaScript to deliver free and easily available classes also animated courses for children interaction that are designed to meet the specific requirements of the audience we are targeting. For backend we will use Laravel. Furthermore, a blogging function will be developed to encourage users to share experiences and build a collaborative educational community.

3.2 Proposed Methodology/System Design

a. Social Considerations:

We are using an agile methodology, which will enable continuous modifications based on input from users. Ensuring the accuracy and relevancy of the content will be guaranteed through collaboration with educators and cybersecurity specialists throughout the development process.

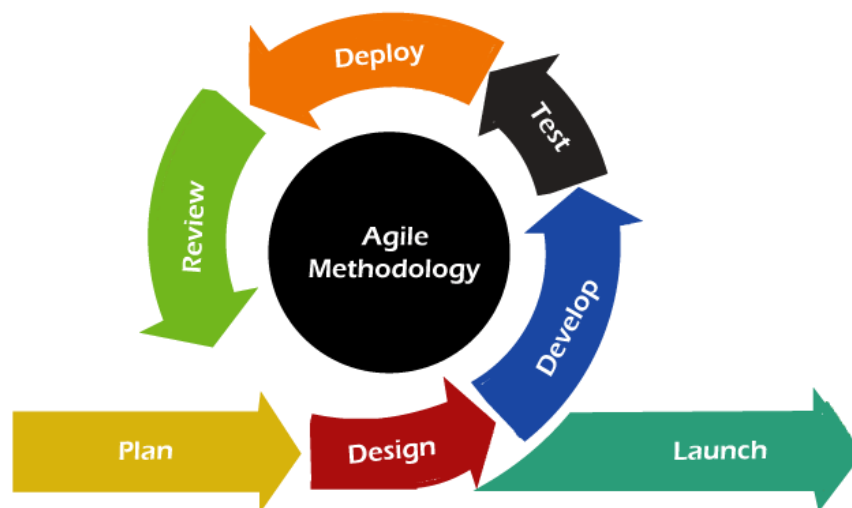


Figure 3.2.0: Agile Methodology

A social assessment will be executed to make sure our content connects to the target audience. In order to include case studies and examples that are suitable for different cultures, interaction with geographic regions cybersecurity experts will be explored. Also, interactive components will be built with our users' most common ways of learning in mind, increasing the platform's relatability and interest.

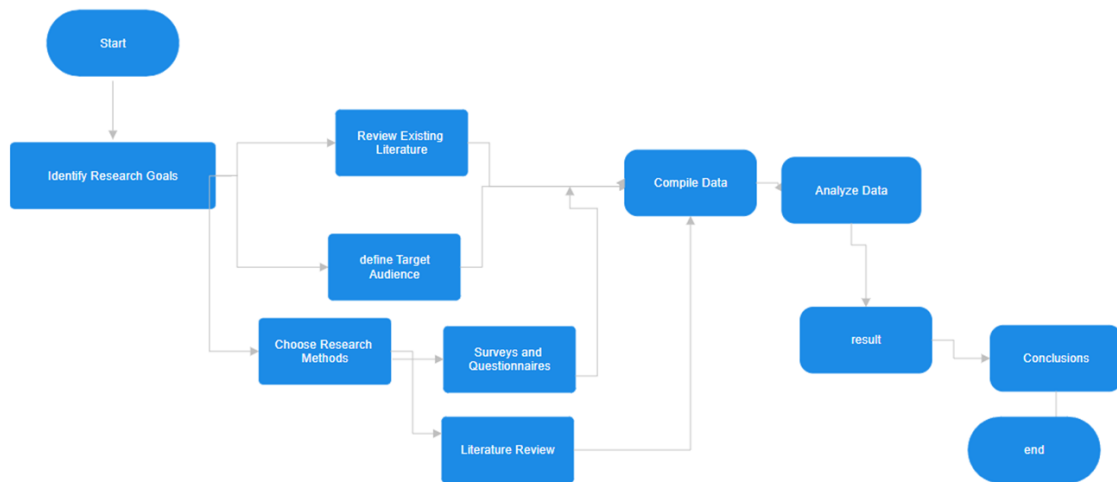


Figure:3.2.1: Methodology of the paper

b. User-Friendly Design: To make navigation simple, the user interface will be created with simplicity and understanding in mind. To satisfy a range of linguistic preferences, there will be different language alternatives available. Additionally, focused elements will enhance the process of learning and keep users motivated to participate in their learning about cybersecurity.

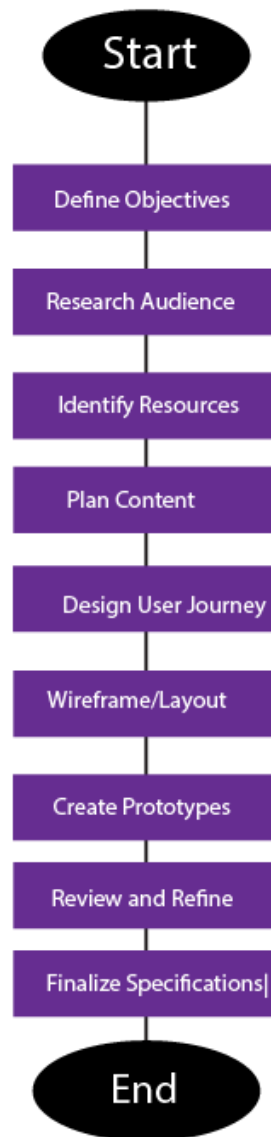


Figure 3.2.2: Website Decision flowchart

First, we outline the objective for which we created this website. We analyze current platforms specialized to women's and children's cybersecurity awareness and perform research to determine the potential audience. We locate educational and blogging resources and carefully select and examine their content, especially Sikho, 10minschoo, and Blog - Bangladesh Cyber Security. We then work on the website's layout and prototype, completing the design in accordance with our goals and research.

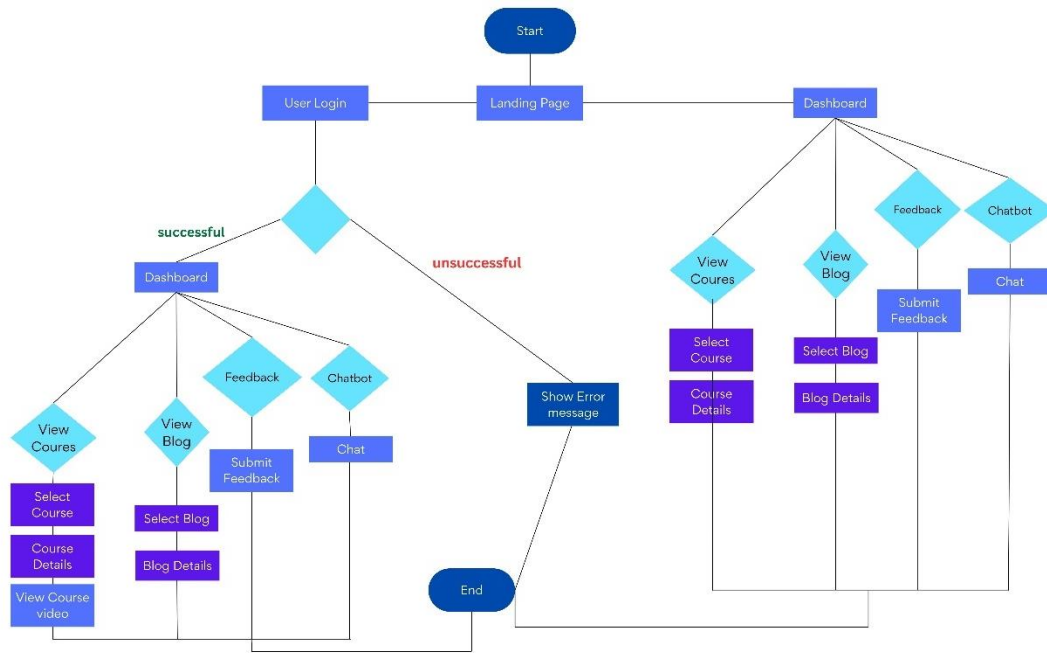


Figure 3.2.3: Website Flow chart for students

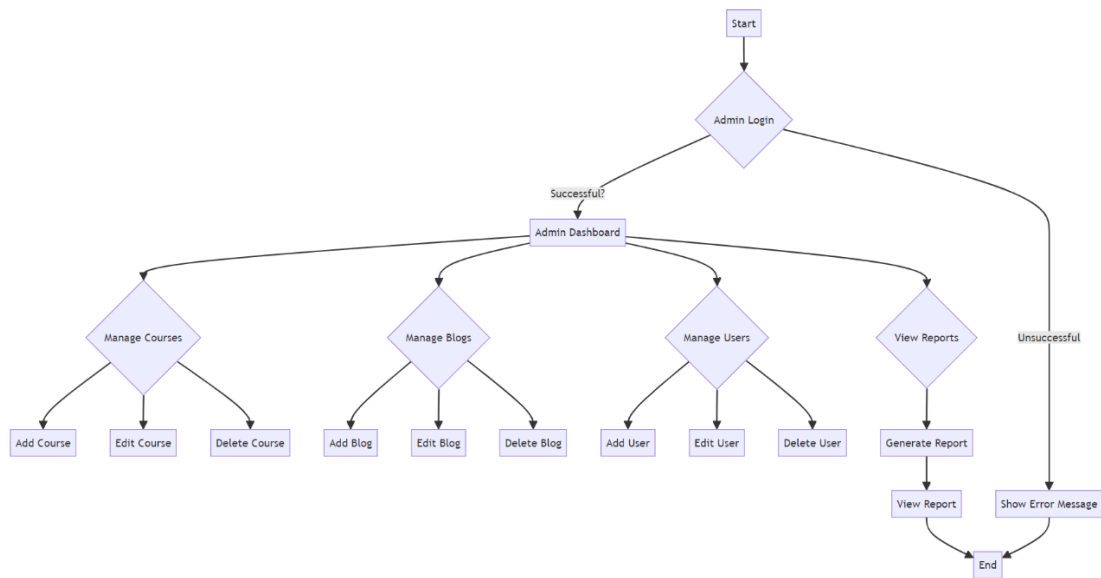


Figure 3.2.4: Website Flow chart for Admin

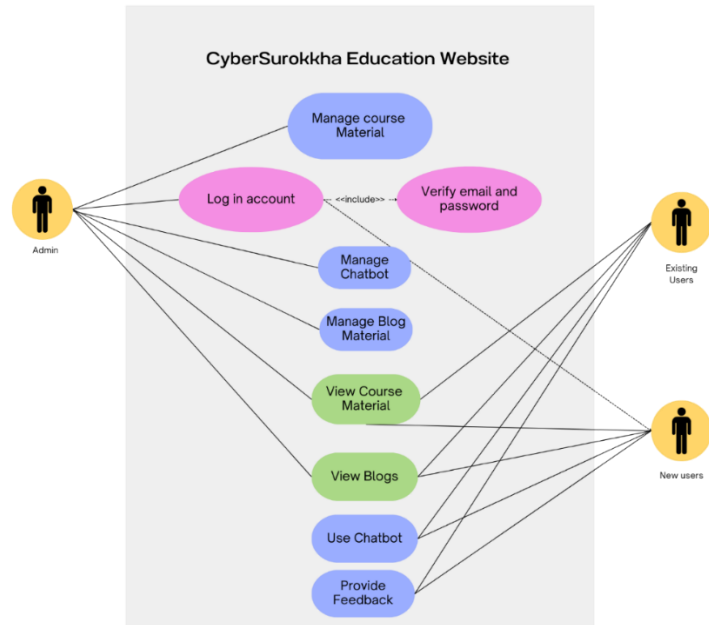


Figure 3.2.5: Website Use case Diagram

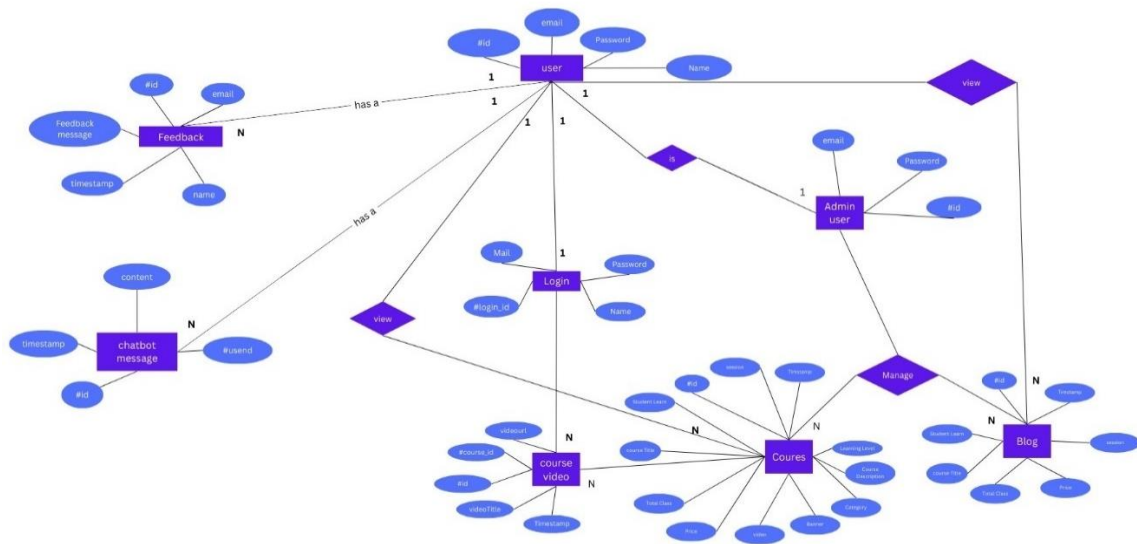


Figure 3.2.6: Website ER Diagram

From the figure 3.2.6 this is the e learning platform “Cybersurokkha” ER Diagram. Visitors start by registering with their name, email, and password. Once registered, users can log in to access additional features. Admin users, who register with an email and

password, have special privileges to manage the site's content.

Admins upload courses with detailed information such as title, description, category, price, total classes, learning objectives, and media including videos and banners. While course details are viewable by all users, only logged-in users can watch course videos. Additionally, admins create and upload blog posts covering various educational topics, complete with titles, descriptions, categories, banners, and timestamps.

Registered users can browse and view detailed information about courses and blog posts. However, watching course videos is restricted to logged-in users. These users can also send messages for support or chatbot interaction, including content, timestamps, and their user ID. Feedback submission is another feature available to logged-in users, allowing them to share their experiences or report issues by providing their name, email, message, and a timestamp.

Admins exclusively handle the uploading and management of courses and blogs. They can add new content, update existing entries, and ensure the information remains relevant. Additionally, admins oversee user activities, handle feedback, and respond to messages, ensuring smooth platform operation.

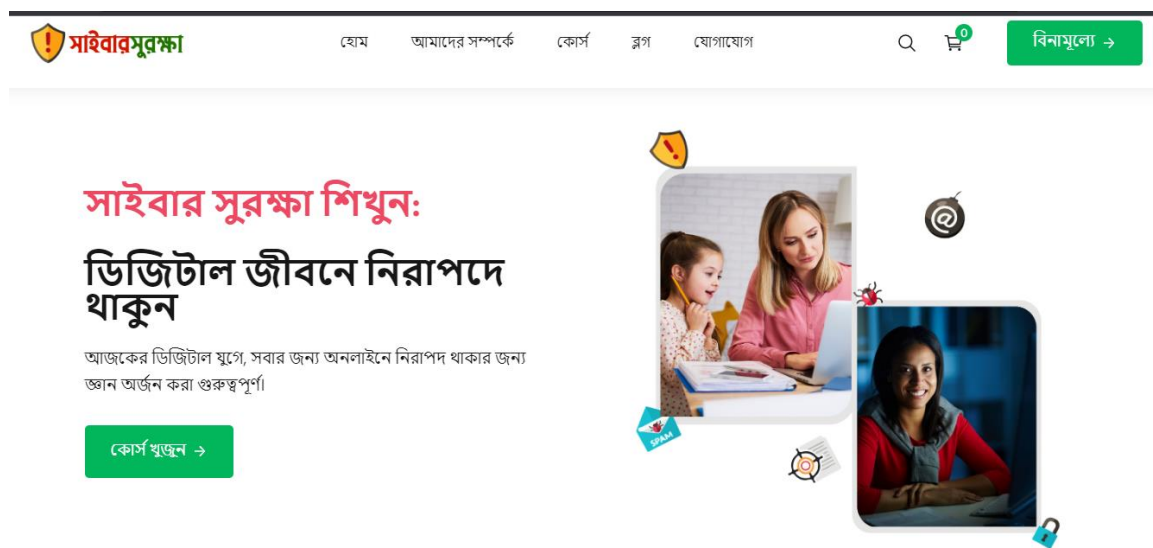


Figure 3.2.7: Website Home page

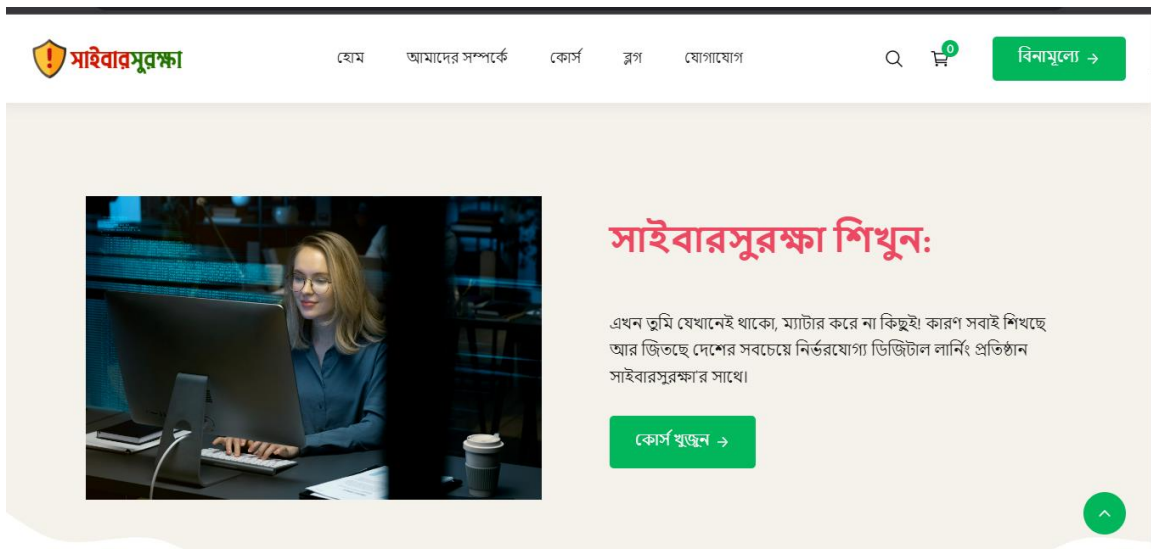


Figure 3.2.8: Website Home page

This page indicates to our home page .

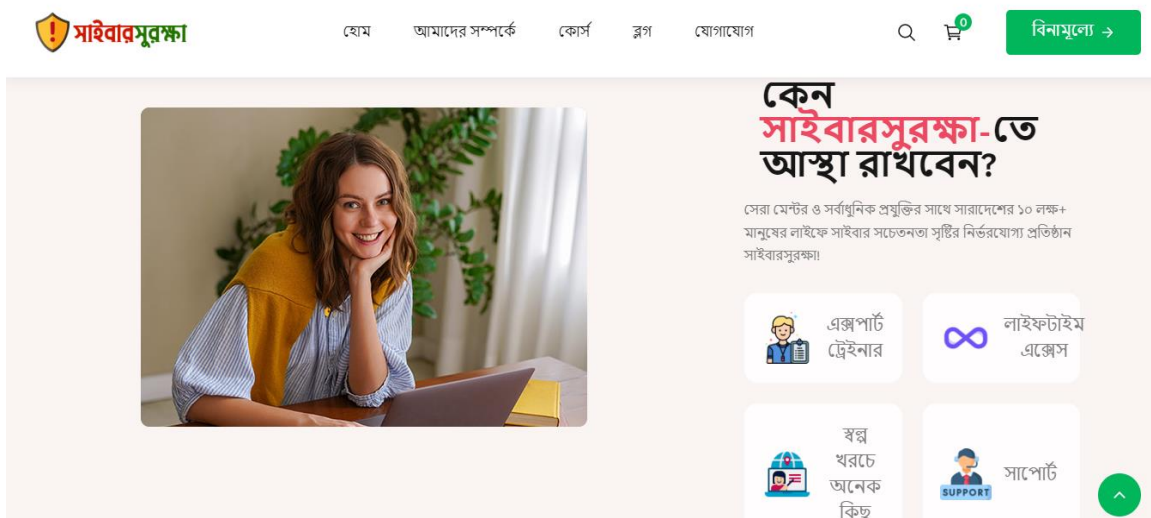


Figure3.2.9: Website Service

Users will be able to get to know about our services.

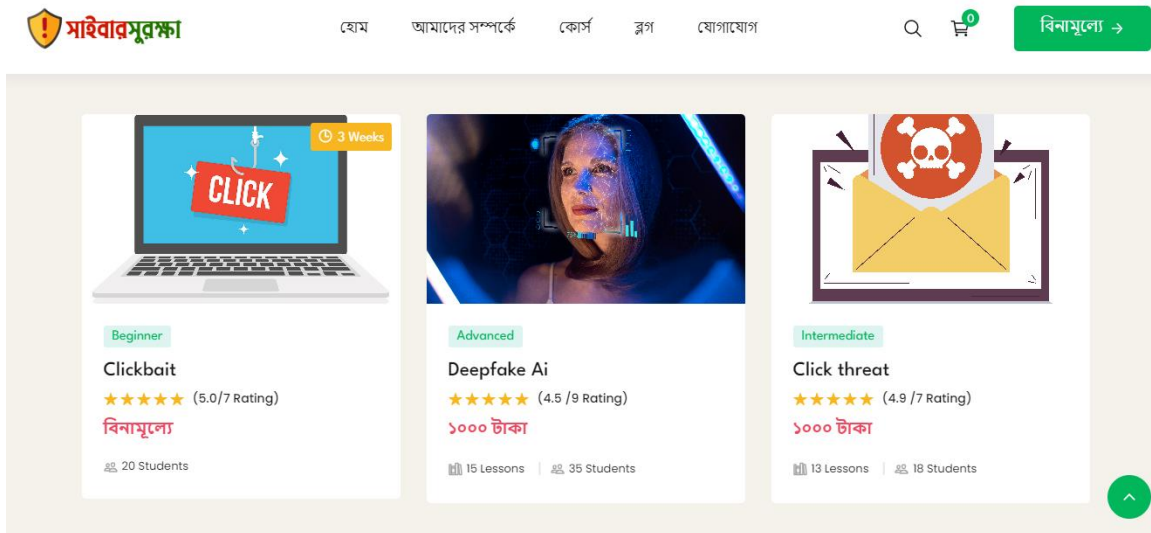


Figure 3.2.10: Awareness course

Users will be able to see the available courses in our platform both in Bangla and English.

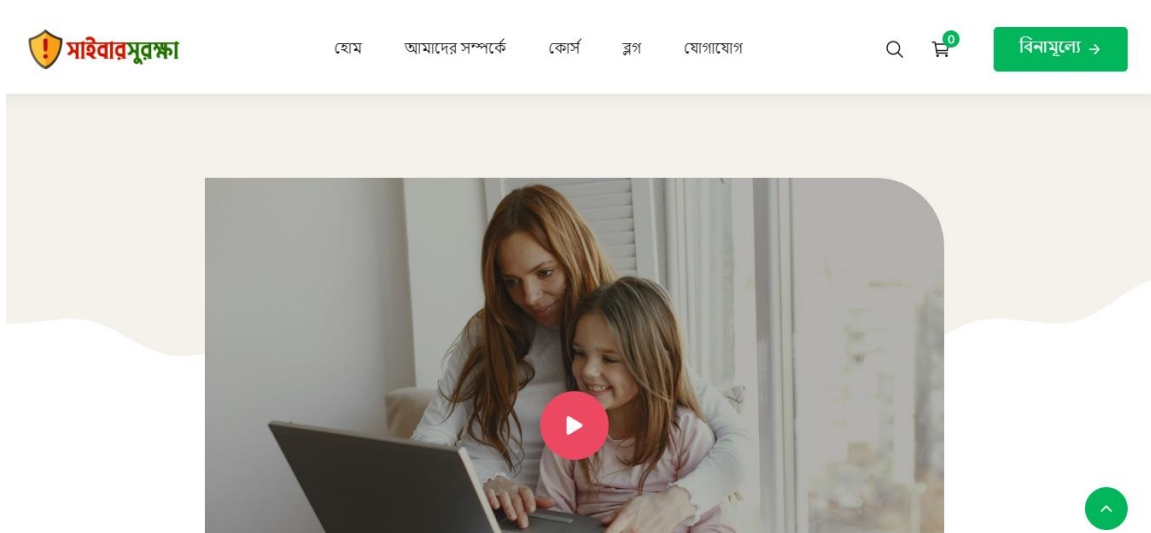


Figure 3.2.11: A video About cybersurokkha

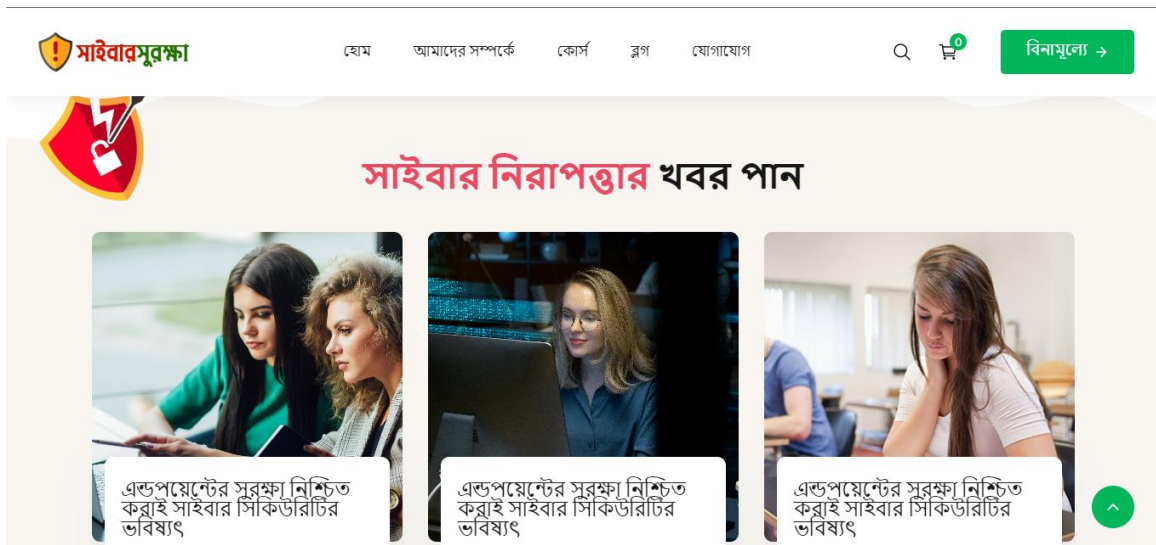


Figure 3.2.12: Blog post section

This section is use for people experience share. Everyone can share their experience.

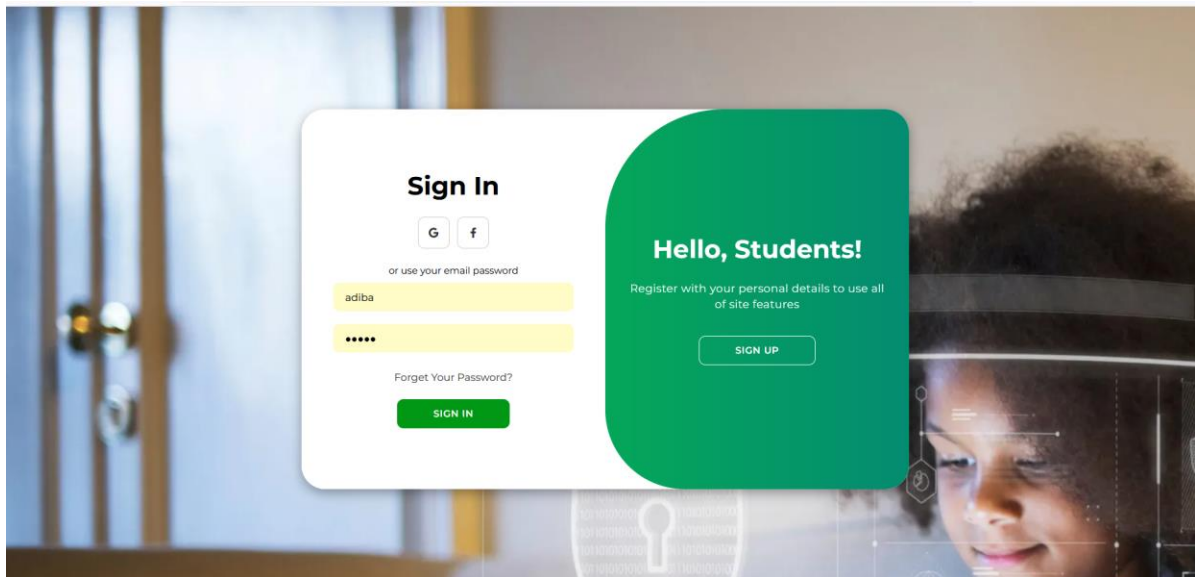


Figure 3.2.13: login page from students

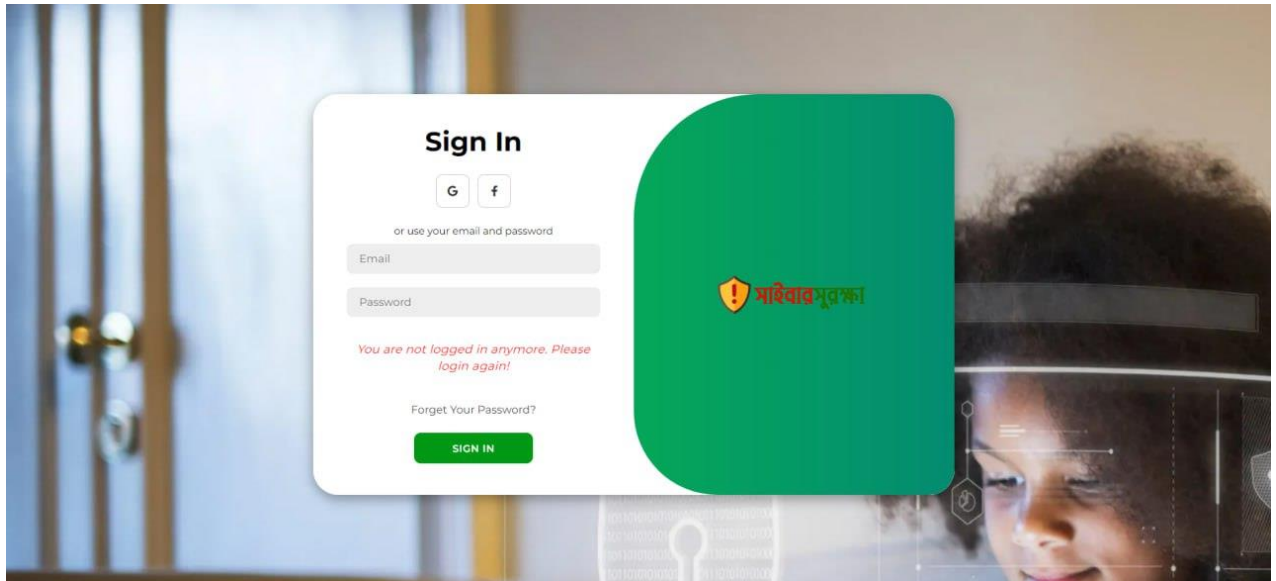


Figure 3.2.14: login page from Admin

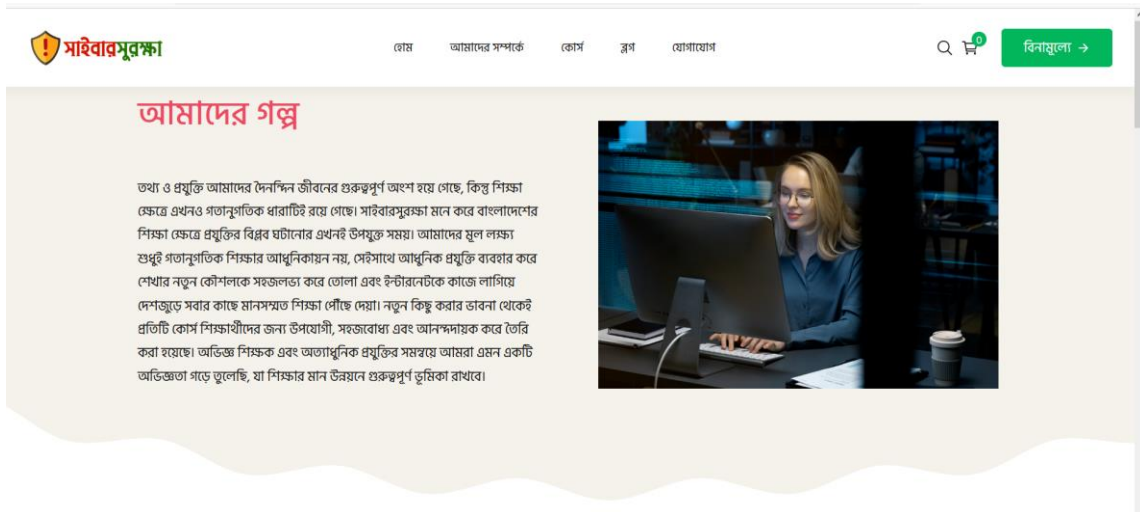


Figure 3.2.15: know About us

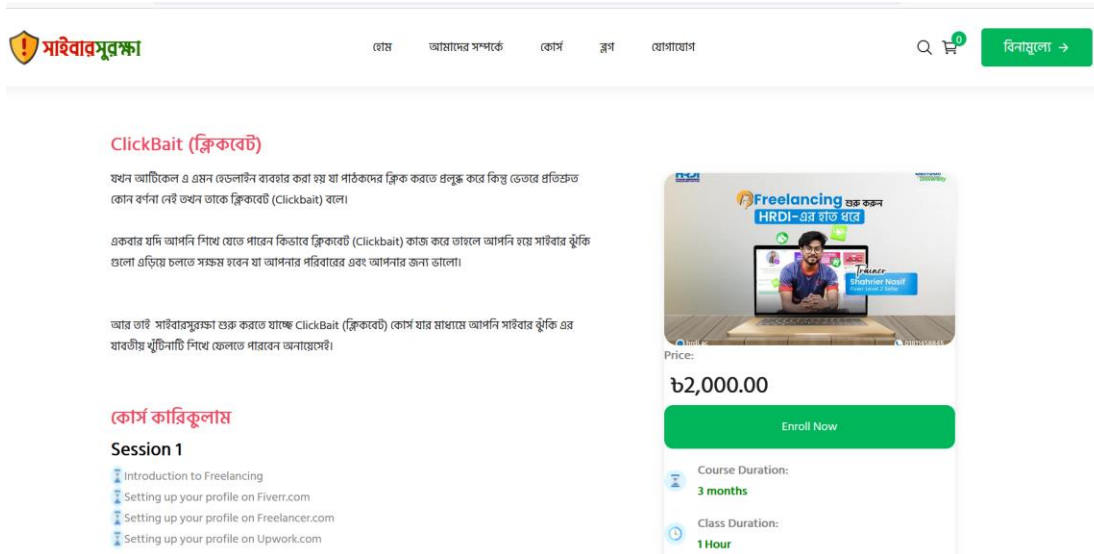


Figure 3.2.16: Single course details page

Figure 3.3.16, We can know the course details and course items also instructor informations.

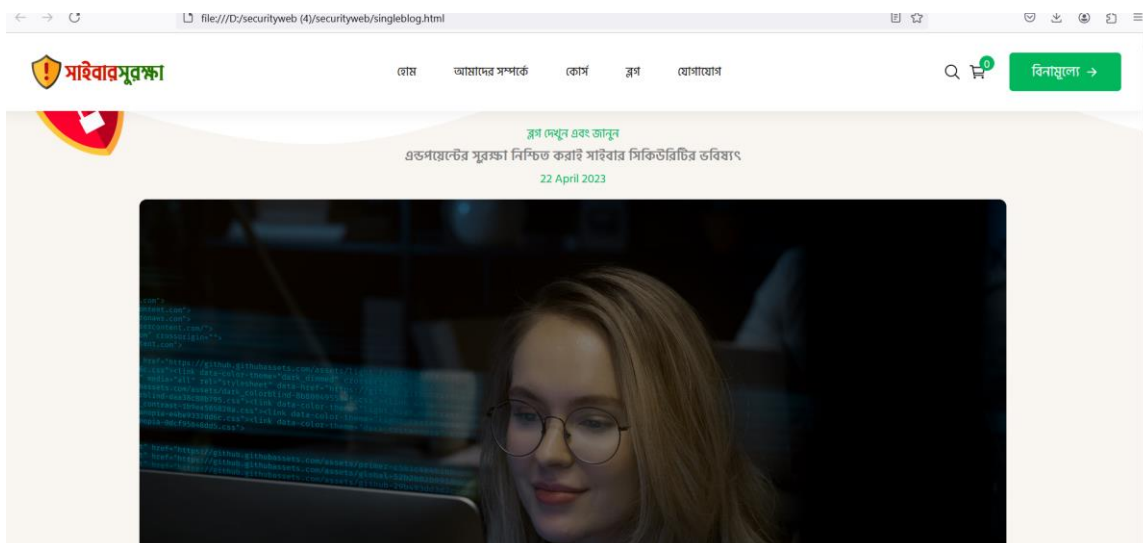


Figure 3.2.17: Single blog page

Figure 3.217 , Everyone can saw the Blog from here .In future we are open it for the subscriber then they can upload the blog the can upload it.

Website Admin Site:

The screenshot shows the 'Add Course' form in the admin interface. The left sidebar contains links to Dashboard, Course (highlighted), Uploaded Course, Blog, and Uploaded Blog. The main content area has a header 'Add Course' and a sub-header 'Enter details of your course'. The form includes fields for 'Course Title', 'Course description', and 'Banner upload' (with an 'Upload Banner Image' button and a 'Banner Upload' button). A 'Select Category' dropdown is set to 'ICT'. At the bottom, there are labels for 'Price' and 'Total Class'.

Figure 3.2.18: For upload the course

The screenshot shows the 'Uploaded Course' table in the admin interface. The left sidebar contains links to Dashboard, Course, Uploaded Course (highlighted), Blog, and Uploaded Blog. The table lists five courses with columns for Course Name, Type, Price, Status, and Action.

Course Name	Type	Price	Status	Action
Building Scalable APIs with GraphQL	Beginner	\$350	Pending	Edit Delete
Bootstrap 5 From Scratch	Intermediate	\$256	Pending	Edit Delete
Graphic Design Masterclass	All level	\$347	Live	Edit Delete
Learn Invision	All level	\$445	Live	Edit Delete
Angular – The Complete Guider	Intermediate	\$165	Live	Edit Delete

Figure 3.2.19: For saw all the uploaded course

Figure 3.2.19 from this figure we can saw that in this page admin can Edit , Delete update the course from this page.

Add Blog

Enter details of your Blog

Blog Title

Blog description

Banner upload

Select Category

Short Description

Figure 3.2.20: For uploaded blog

Figure 3.2.20: from this figure we can saw that in this page admin can Edit , Delete update the blog from this page.

Courses

SEARCH YOUR DESIRED COURSE

Please enter a search query.

Figure 3.2.21: search box

3.3 Hardware/ Software Requirement

3.3.1 Front-end

“সাইবারসুরক্ষা” – Web based cyber awareness program" has a front-end design that emphasizes a contemporary, user-friendly interface. It makes use of responsive design concepts for seamless cross-platform use. The user interface (UI) has an intuitive structure that facilitates effortless navigation and expedient access to essential functions including blogs and course pages with prices and free courses, controlling administration, and customized user profiles. User engagement is improved by chat bot(Under developed). To guarantee a positive and effective user experience, the design places a high priority on accessibility, usability, and aesthetics.

3.3.2 Back-End

“সাইবারসুরক্ষা” – Web based cyber awareness program" back-end architecture makes use of PHP , using Composer for package management, and PHP artisan as a command-line tool for efficient development.

Its MVC framework and modular design allow the smooth integration of several functionalities. Installing and maintaining project-specific packages is made easier using Composer, a PHP dependency management that promotes effective development workflows.

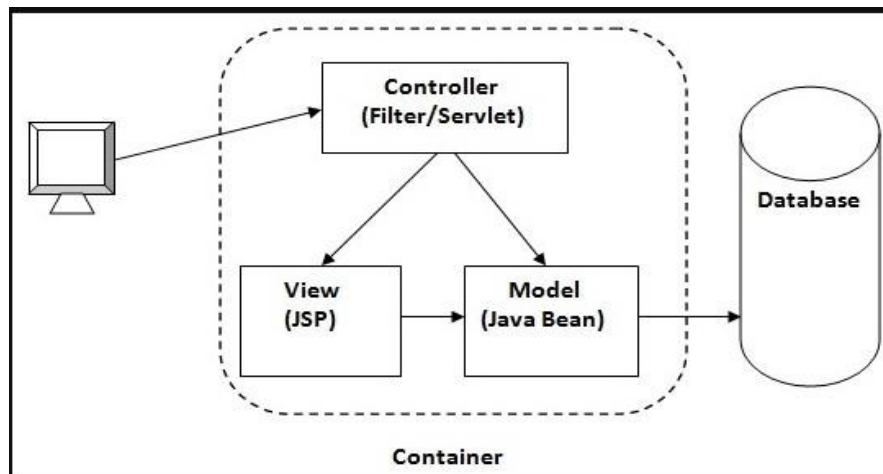


Figure 3.3.1: MVC Architecture.

PHP artisan, increases developer efficiency by automating tedious operations like seedings, database migrations, and component creation. It facilitates efficient code scaffolding, streamlines database administration, and provides user-friendly testing environments.

"সাইবারসুরক্ষা" gains from streamlined development, effective database handling, secure authentication, and robust testing capabilities through Laravel's ORM (Object-Relational Mapping) and its ecosystem of libraries and tools, helping to create a stable, scalable, and maintainable web-based travel management system.

3.4 Project Management and Financial Analysis

Project Management and Finance

Project Objectives:

- To develop a ecommerce website for buy and sell agricultural products
- To give an one stop solution for consumers of agricultural products
- To provide a platform for farmers to sell their product directly to their customers.

• Project Timeline:

A. Phase 1: Project Planning and Research (2-4 weeks)

B. Phase 2: Design and Prototyping (6-8 weeks)

- C. Phase 3: Front-End Development (8-11 weeks)
- D. Phase 4: Back-End Development (10-15 weeks)
- E. Phase 5: Testing (4-6 weeks)
- F. Phase 6: Deployment (2-5 weeks)
- G. Phase 7: Post-Launch and Marketing (Ongoing)

Resource Planning:

A. Equipment and Tools:

- Development and Testing Servers
- High-performance Computers for Development Team Design Software (e.g., Adobe Creative Suite)
- Collaboration Tools (e.g. Trello)
- Version Control System (e.g. Git)
- Testing Tools (e.g., Selenium for automated testing)

B. Software and Technologies:

- Front-End Technologies (e.g., HTML, CSS, JavaScript, React or Angular)
- Back-End Technologies (e.g., Node.js, Django, Flask, or Ruby on Rails)
- Database Management System (e.g., MySQL)
- Server Hosting (e.g., AWS, Azure, or Google Cloud)
- Payment Gateway Integration (e.g., Bkash, Nagad, PayPal)
- Security Software and SSL Certificates

C. Data and Content:

- Product Data: Provided by sellers or sourced through agricultural databases/APIs
- Product Images: Provided by sellers or obtained through agreements with suppliers
- User Documentation: Prepared by the technical writing team

D. Training and Skill Development:

- Ensure that the development team has the necessary training and skills in e-commerce development, security, and database management.
- Provide additional training on specific technologies and tools as needed.

Communication Plan:

A. Stakeholder Meetings:

Purpose: Update stakeholders on project requirements gathering progress and gather feedback.

Participants: Team members, and stakeholders.

Frequency: Bi-weekly or as specified in the project plan.

B. Change Control Meetings:

Purpose: Discuss and approve any changes to the project scope or requirements.

Participants: Supervisor, and team members.

Frequency: As needed when change requests arise.

Financial Analysis:

A comprehensive cost-benefit evaluation that take into account prospective partnerships, ongoing maintenance, and development costs will be carried out. To maintain the platform's development, its top concern will be looking into funding options via grants, sponsorships, or partnerships with relevant groups.

A general table with estimated costs for different components of a web development project. So, here is the estimated table based on our requirements.

TABLE 3.4.1: Estimated Cost for Web Development Project

SN	Components	Estimated Cost (BDT)
01.	Domain and Hosting	1500-2000
02.	Purchase Stock Content	1600-2000
03.	Visiting Stakeholders	500-1000
04.	Doing Online Course or Training for learning new technology	2000-3000
06.	Documentation and Report Writing	1000-1500
05.	Miscellaneous (e.g., licenses, tools)	3000-4000
06.	Contingency (10% of total)	900-1300
	Total Estimated Cost	11,400-14,800

3.5 Summary

Our goal is to develop an online platform on cybersecurity awareness targeting the women of Bangladesh and parents where we will use HTML, CSS, JavaScript, and Laravel for the backend. It will have Basic classes as free classes, animated classes for kids, and a blogging section to write the experience gained.

Specific Needs: Determine needs regarding cybersecurity of the target audience with the help of surveys, interviews, and researches. Technical Requirements: Make sure it will have secure authentication, easy to manage and nice interface, working well on multi-devices, and ability to host videos.

Social Considerations: Use the agile development approach to implement iterations, engage teachers and IT specialists, as well as, use culturally sensitive materials and such elements as games.

User-Friendly Design: Concentrate all the information in the center of the screen to make it potential and facilitate better learning of people since we are targeting to help multiple international people; The user interface shall thus be designed in a way that reflects simplicity and ease of use The language used on the interface shall also be multiple since it will target multiple international people.

Project Management and Accounting

Project Objectives: devise an e-commerce venture for agricultural produce by creating an outlet for the farmers' produce.

Project Timeline: The examples are the planning stage, the designing phase, the front end and back end development stage, and testing, deployment, and follow-on-formation stages.

Resource Planning: Test platform: development servers, high profile PCs, designing tools, collaboration and version control, and testing instruments.

Financial Analysis: Perform a SWOT analysis to identify and estimate costs for the domain, hosting, content, training and miscellaneous which costs BDT 11,400 – 14,800.

CHAPTER 4

IMPLEMENTATION

4.1 Overview

“Cyber Security Awareness for Parents and Women Perspective” is a project that uses a systematic method of evaluating and improving the level of cyber security knowledge among parents and women. It relies on Google Forms as the channel of data collection with an aim to gain insights into their participants’ cyber security habits, awareness levels and some demographics. In this case, Google Colab is used in data analysis whereby Pandas are employed in doing preprocessing to allow extraction of metrics like taking part in awareness programs and risk assessments.

Website development has been done through Visual Studio using HTML, CSS, JavaScript, PHP providing convenient user interfaces for collecting information from users securely sent to MySQL database managed by XAMPP. The survey forms have been integrated into deployment strategies ensuring accessibility and functionality.

The study findings highlight the significance of formal education and parental roles in forming children’s cybersecurity practices. They point out areas where improvement is needed such as weak password management or unawareness program participation especially among women. Besides, ethical issues are also covered where research process emphasizes on privacy issues while always obtaining informed consent from all subjects involved. As a whole, this comprehensive approach aims at equipping parents as well as women with essential knowledge plus tools required for effective navigation within the online environment which is considered safe.

4.2 Train Model/ Prototype Design

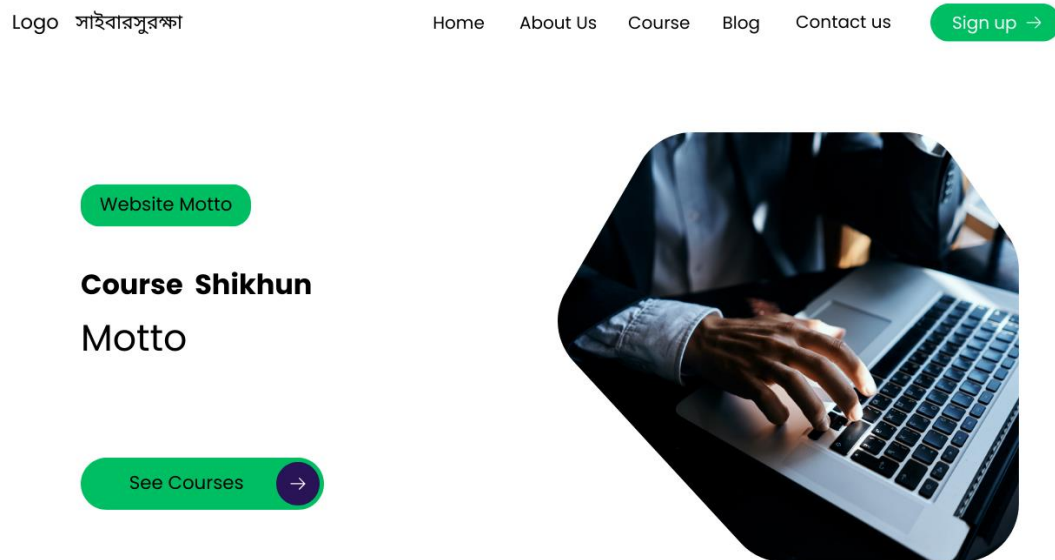


Fig: 4.2.1 Prototype design home page

Figure 4.1.1 shows the prototype design of the home page before Login

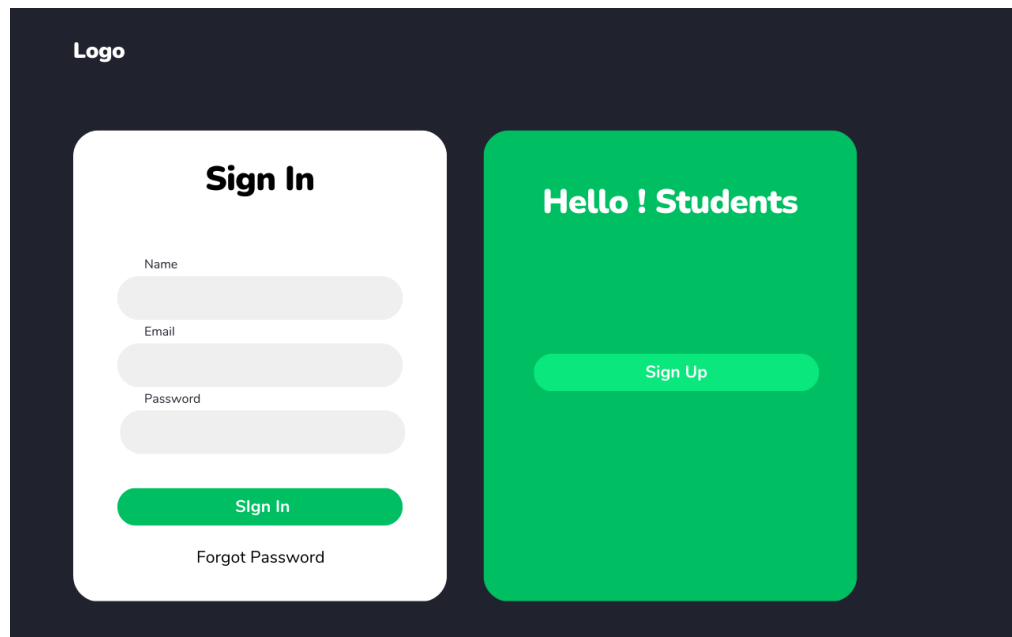


Fig: 4.2.2 Prototype design of login and signup page

Figure 4.1.2 shows the prototype design of sign up and sign in page of the website
©Daffodil International University

Running Courses

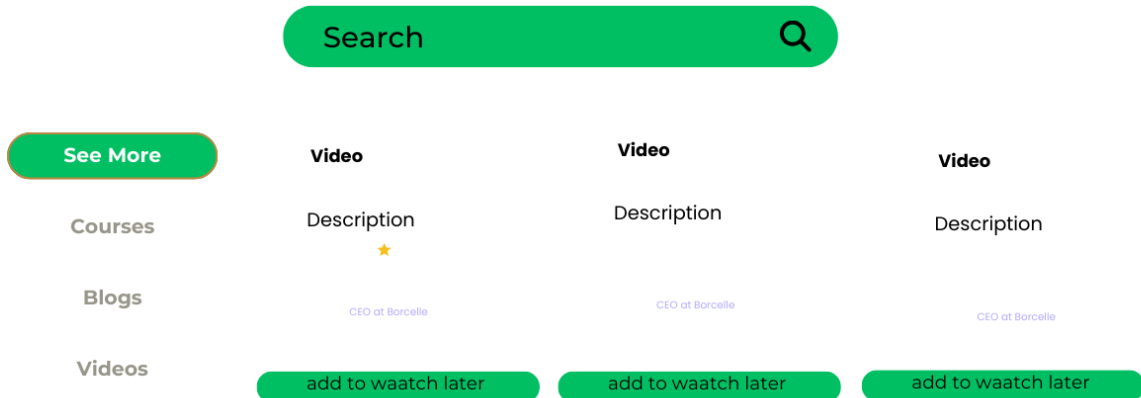


Fig: 4.2.3 After login homepage prototype design

Figure: 4.2.3 shows the home page prototype after login

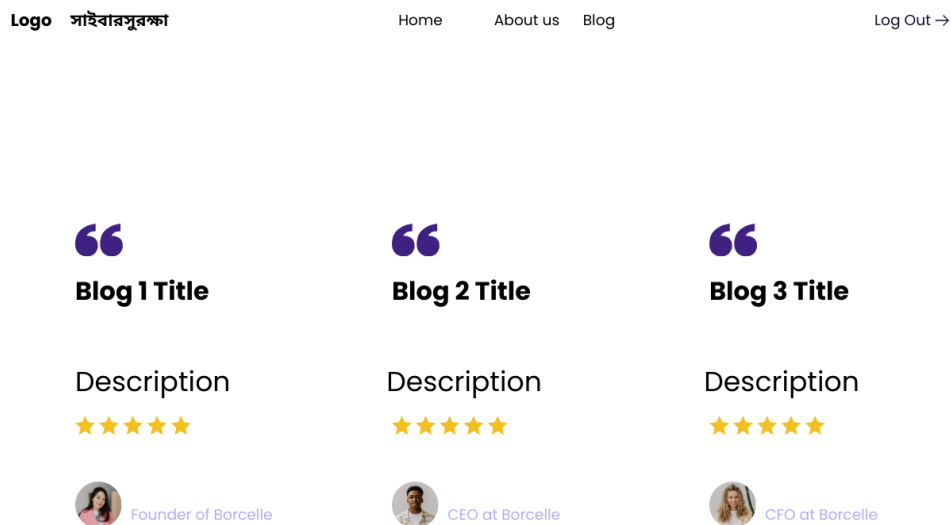


Fig: 4.2.4 Blog page prototype design

Figure 4.1.4 shows the how the blogs will be shown

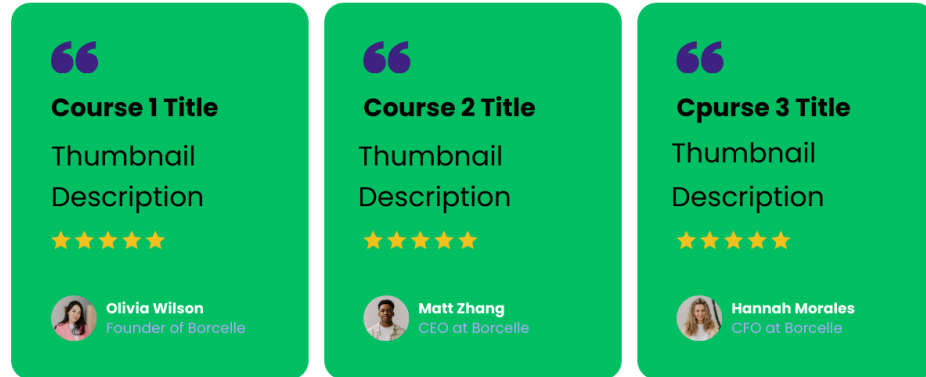


Fig: 4.2.5 Course page prototype

Figure 4.2.5 shows the prototype page design of course page.

Course Title

Description

About Course

- 1
- 2
- 3

Thumbnail

Price 2000

Enroll Now

Fig: 4.2.6 Course details page prototype

Figure 4.1.6 shows the prototype design of the course details page

4.3 System Testing/ Model Evaluation

Showing rows 0 - 3 (4 total, Query took 0.0010 seconds)

[SELECT * FROM `blogs`](#)

[Profiling](#)
[\[Edit inline \]](#)
[\[Edit \]](#)
[\[Explain SQL \]](#)
[\[Create PHP code \]](#)
[\[Refresh \]](#)

☐ Show all |
 Number of rows: |
 Filter rows: |
 Sort by key:

[Extra options](#)

		id	blogTitle	blogDescription	banner	category	shortDescription	created_at
1	Edit Copy Delete	1	ভোটা চুরি আমাদের নিরাপত্তা হুমকির সম্মুখীন	ভোটা চুরি কী? ভোটা চুরি হলো একটি সাইবার আক্রমণ যেখানে যাকার...	blog-3.jpg	Cyber Security	ভোটা চুরি হলো একটি সাইবার আক্রমণ যেখানে যাকার...	2024-05-23 00:45:33
3	Edit Copy Delete	3	কিশি: আক্রমণ কিভাবে চিনবেন এবং প্রতিহত করবেন	কিশি: আক্রমণ কী? কিশি: আক্রমণ সাধারণত হুমেলি বা এ...	course-1.webp	Cyber Security	কিশি: আক্রমণ সাধারণত হুমেলি বা এস.এম.এস ব্যবহার করে ...	2024-06-28 18:45:44
5	Edit Copy Delete	5	রহানসমওয়ার আক্রমণ কিভাবে সুরক্ষিত থাকবেন	রহানসমওয়ার কী? রহানসমওয়ার একটি ধরনের মা...	./assets/images/blog-1.jpg	Mobile App	রহানসমওয়ার একটি ধরনের ম্যালওয়্যাস যা আপনার ...	2024-06-28 18:54:12
7	Edit Copy Delete	7	ডিপফেক: এআই কী? প্রতিদ্বন্দ্বি	ডিপফেক: এআই হল এক ধরনের কৃত্রিম বুদ্ধি...	./assets/images/course-2.jpg	Cyber Security	ডিপফেক: এআই হল এক ধরনের কৃত্রিম বুদ্ধিমান (AI) ...	2024-06-28 20:03:55

Fig: 4.3.1 Shows the chatbot input data

Figure 4.3.1 shows how database is taking inputs from the chatbot. Here the test case is successful. Database can take the trained questions and answers of the chatbot flawlessly.

[illegible]

Fig: 4.3.2 Course input Data

Figure 4.3.2 shows how database is taking inputs from the admin. Here the test case is successful.

		id	name	email	password
☐	 Edit  Copy  Delete	2	sales	sales@weeprint.com	\$2y\$10\$3cb65f7Zim7aPCbN.MBquccthrL73VYkiyqSqPwR0...
☐	 Edit  Copy  Delete	4	Adiba zaman chowdhury	adiba15-3924@diu.edu.bd	\$2y\$10\$dMPdWQ0cRVUkJCjVZCAd..vmS/YwwJov8LuXnHSM00i...
☐	 Edit  Copy  Delete	5	Farhan Adnan	Farhan15-3919@diu.edu.bd	\$2y\$10\$0kdjXOyhsZnN1Q4QOmeieN1AgDGxX6Fyg4ER6zRtNX...

Fig: 4.3.3 Admin input Data

Figure 4.3.3 shows how database is taking inputs from the admin (username & Password). Here the test case is successful.

		id	name	email	message	created_at
☐	Edit	2	Adiba zaman chowdhury	adiba15-3924@diu.edu.bd	need to improve more	2024-06-28 21:16:15
☐	Edit	3	Farhan Adnan	Farhan15-3919@diu.edu.bd	Good website help for the cyber awareness	2024-06-28 23:51:07

Fig: 4.3.4 User Data Input

Figure 4.3.4 shows the user input data table where we can see the suggestions of the users

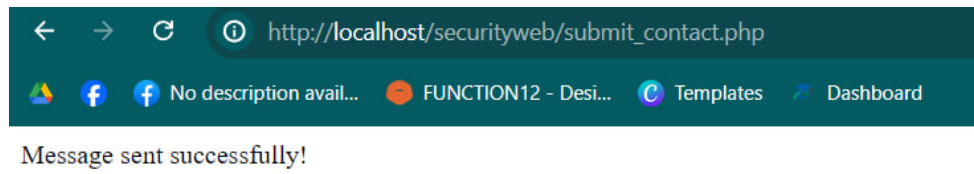


Fig: 4.3.5 Message store Database

Figure 4.3.5 shows the chatbot input data. Is shorted the database successfully

Extra options

  					id	content	
☐		Edit		Copy		Delete	1 hi
☐		Edit		Copy		Delete	2 hi
☐		Edit		Copy		Delete	3 hi
☐		Edit		Copy		Delete	4 hi
☐		Edit		Copy		Delete	5 cyber security
☐		Edit		Copy		Delete	6 cyber security
☐		Edit		Copy		Delete	7 I'm sorry, I don't have information on that topic.
☐		Edit		Copy		Delete	8 cyber security
☐		Edit		Copy		Delete	9 I'm sorry, I don't have information on that topic.
☐		Edit		Copy		Delete	10 ok
☐		Edit		Copy		Delete	11 I'm sorry, I don't have information on that topic.
☐		Edit		Copy		Delete	12 ok
☐		Edit		Copy		Delete	13 I'm sorry, I don't have information on that topic.
☐		Edit		Copy		Delete	14 cybersecurity
☐		Edit		Copy		Delete	15 Cybersecurity in Bangladesh is improving with new ...
☐		Edit		Copy		Delete	16 bangladesh
☐		Edit		Copy		Delete	17 Bangladesh is working towards better cybersecurity...
☐		Edit		Copy		Delete	18 bangladesh
☐		Edit		Copy		Delete	19 Bangladesh is working towards better cybersecurity...
☐		Edit		Copy		Delete	20 bangladesh
☐		Edit		Copy		Delete	21 Bangladesh is working towards better cybersecurity...
☐		Edit		Copy		Delete	22 bangladesh

Figure 4.3.6: chatbot data store table

Figure 4.3.6 shows the chatbot input data. From this, we can understand what the user wants to know, allowing us to train our website with this data.

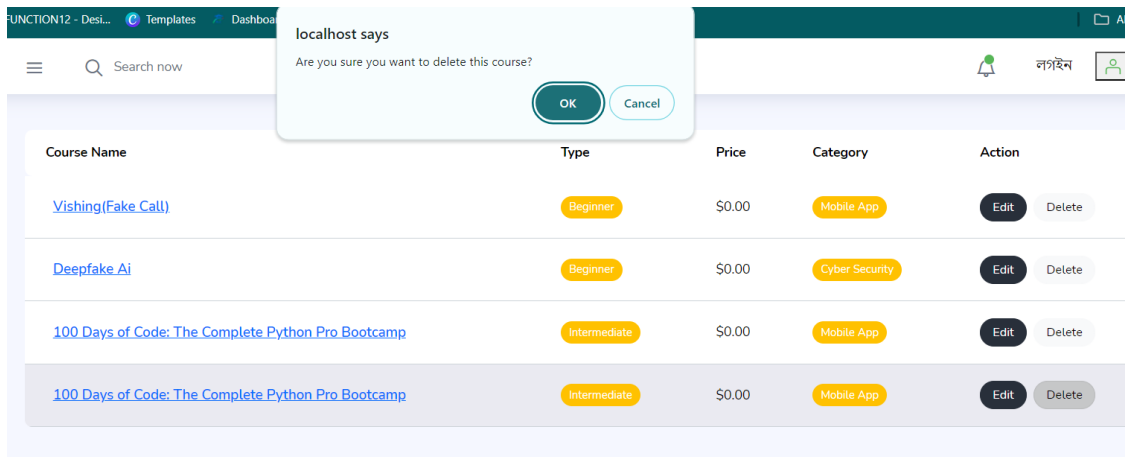


Figure 4.3.7: Delete course from database

Figure 4.3.7 shows that delete the course from the database

4.4 Summary

In these chapter we have showed the prototype we designed for our website and how the inputs in out database is working. We input courses and blogs and it processes in the database and the results have been attached. In Fig (4.1.1 – 4.1.6) the prototype design had been shown and In Fig (4.2.1-4.2.5) testing had been shown and how the database is working. We tried to have a healing color like green for the UI , because green is color of healing. That's why we tried to have the combination of green and white and in some places green and black.

CHAPTER 5

RESULT AND ANALYSIS

5.1 Overview

This challenge ambitions to decorate cybersecurity focus amongst dad and mom and women by way of leveraging information series, evaluation, and academic equipment. A Google Forms survey will gather facts on cybersecurity behavior and consciousness, with responses exported to Excel for evaluation in Google Colab. The records could be preprocessed and analyzed to derive key insights. A website, advanced using HTML, CSS, JavaScript, and PHP, will gather and percentage records. It will function person-friendly interfaces, interactive forms, and records visualizations. Ethical considerations will make sure privacy and consent. The intention is to improve cybersecurity practices via schooling and knowledgeable techniques, fostering a safer on-line surroundings.

5.2 Experimental/ Simulation Result

This setup describes the process for examining "Cyber Security Awareness for Parents and Women Perspective". Google Colab is utilized for data analysis, while a website is crafted using Visual Studio with HTML, CSS, JavaScript, and PHP for data gathering and sharing.

To start with, data must be collected. A survey employing Google Forms should be designed to gather information from parents and women regarding their cybersecurity habits and awareness. Questions should cover participation in awareness programs, the perceived effectiveness of such programs, use of security measures like two-factor authentication, and demographic details. The survey responses should then be exported to an Excel file for further examination.

Moving on to Data Preparation and Analysis in Google Colab entails importing the Excel file into Google Colab to load it into a Pandas DataFrame. It is crucial to inspect the data structure for missing values and preprocessing necessities appropriately.

For Data Preprocessing, missing values should be handled using relevant strategies (e.g., mode for categorical columns), irrelevant columns dropped, and columns renamed for clarity.

Data Analysis involves calculating awareness metrics for parents, women, and children based on survey responses. Key metrics include total participants in awareness programs, program effectiveness ratings, and impacts on children's awareness levels stemming from parental cybersecurity practices. Risk levels associated with current practices among parents and women should also be assessed.

Website Development plays a critical role in data collection and distribution solutions. Front-End Development involves structuring web pages with HTML, styling with CSS , Bootstrap for user-friendly interfaces, while adding interactivity with JavaScript like form validations.

Back-End Development includes crafting server-side logic using PHP to handle form submissions and engaging with databases via XAMPP for local testing environments.

Database Management necessitates setting up a MySQL database using XAMPP to store survey data efficiently while designing schemas that ensure swift data retrieval.

Integration & Deployment guidelines suggest embedding surveys on the website through Google Forms or crafting custom forms using HTML/JavaScript integrated with PHP to manage submissions securely in MySQL databases. Visualizations using libraries like Chart.js or Javascript can vividly represent results on the site to educate users about cybersecurity trends.

Ethical Considerations dictate that all activities adhere to ethical standards respecting user privacy rights by anonymizing data for participant protection while seeking informed consent always.

Finally, Documentation & Reproducibility stress detailed transcripts of codes used in “Google Colab” alongside clear documentation about website development processes in

terms of design features & functionalities ensuring transparency in sharing methodologies facilitating future research endeavors effectively. This methodology enriches the understanding of cybersecurity preparedness among parents & women through meticulous data analysis via “Google Colab” & a comprehensive web solution aiding effective information dissemination.

We have used some survey questions to get the data and information we need for this project .

Research Questions

The survey questions serve to enhance the paper "Cyber Security Awareness for Parents and Women Perspective" cybersecurity awareness among women and parents by focusing on specific areas that impact their online safety practices. Here's the significance of each question set:

The survey queries aim to enhance cybersecurity awareness among women and parents by focusing on specific aspects that impact their online safety. Each set of questions holds significance for the following reasons:

1. Demographic Information:

- a) Are you a parent?**
- b) Are you a woman?**
- c) What is the age of your child?**
- d) What is the age of you?**
- e) How frequently does your child use the internet?**
- f) What internet device you have?**
- g) How do you connect to the internet?**
- h) What is your education level?**

• Identification of Parents and Gender:

- Recognizing respondents as parents or women aids in customizing cybersecurity resources for these groups, considering their distinct vulnerabilities and requirements.

- **Age and Internet Usage:**
 - Insight into the age of respondents and their children, along with internet usage patterns, facilitates a better grasp of potential risks and the design of age-appropriate educational materials.
- **Devices and Connectivity:**
 - Data on devices utilized and internet connection supports in pinpointing potential security gaps and areas necessitating enhanced protection.
- **Education Level:**
 - Awareness of respondents' education levels assists in developing educational programs accessible to a broad audience.

2. Cybersecurity Knowledge:

a) How confident are you in your knowledge of common cyber threats?

b) Have you or someone you know ever experienced a cyber threat or attack?

- **Confidence and Experience:**
 - Evaluating confidence in cybersecurity knowledge and previous encounters with cyber threats helps gauge awareness levels and identify areas requiring further education.

3. Awareness and Education:

a) Have you participated in any cybersecurity awareness programs or workshops specifically designed for parents or women?

b) how effective do you think these awareness programs are in educating about cybersecurity threats?

- **Participation in Programs:**
 - Queries related to involvement in cybersecurity programs and their efficacy offer insights into the extent and impact of existing awareness initiatives. This aids in recognizing shortcomings and enhancing future programs.

4. Common Practices:

a) Does your child know how to create strong and unique passwords for online accounts?

b) How often do you remind your child not to share personal information online?

- **Security Measures:**

- Exploration of practices like password updates and two-factor authentication usage discloses the effectiveness of basic security measures. This data is crucial for designing interventions to enhance these practices.

5. Online Behavior:

a) Does your child ask for permission before downloading or installing apps or games?

b) How familiar is your child with the concept of "stranger danger" online?

- **Sharing Information & Verification:**

- Examining the frequency at which respondents share personal information online and verify email authenticity highlights risky behaviors warranting targeted education.

6. Educational Resources :

a) Are there specific online resources or games that your child uses to learn about online safety?

b) How effective do you find these resources in teaching your child about cybersecurity?

For women and parents, these resources are particularly important because they help them guide and educate children about safe online behavior in an age-appropriate manner. They provide structured content that can facilitate conversations about cybersecurity and empower both parents and children to navigate the digital world safely.

8. Cybersecurity & Suggestions for Improvement:

a) Has your child ever encountered a cyber threat or inappropriate content online?

b) If yes, how did your child handle the situation? (Open-ended)

- **Resource Needs:**

- Soliciting suggestions for additional resources garners direct input from the target demographic, aiding in creating more efficient, user-friendly cybersecurity tools, and educational materials.

9. Children's Cybersecurity:

a) What additional support or information do you think would enhance your child's cybersecurity awareness? (Open-ended)

- **Children's Education & Practices:**

- Emphasis on children's formal education in cybersecurity, comprehension of threats, and parental involvement ensures both parents & children are well-prepared to mitigate online risks, fostering a safe digital environment for the entire family.

By addressing these areas comprehensively, the survey efficiently evaluates & bolsters cybersecurity awareness among women & parents, resulting in enhanced protection against cyber threats.

Now the results we gain from the surveys are presenting below :

Result of Experiment 1: Childs' Awareness

TABLE 4.2.1: Childs' Awareness Table

Child	0	1	2	3	4
Age Group	12-18 years	5-11 years	16-18 years	16-18 years	16-18 years
Formal Cyber Education	Yes	No	Yes	No	Yes
Rate Understanding Threats	5	1	5	3	5
Monitor Online Activities	Very actively	Occasionally	Moderately actively	Occasionally	Occasionally
Discussed Cyber Safety	Yes	No	Yes	Yes	No
Know Strong Passwords	Yes	No	Yes	Yes	Yes
Remind No Share Info	Very often	Rarely	Occasionally	Rarely	Occasionally
Familiar Stranger Danger	2	1	5	3	5
Ask Permission For Apps	Always	Never	Never	Never	Sometimes
Online Safety	Yes	No	No	No	Yes

Child Age and Cyber Education

Children aged 5-11 and 16-18 are the focus of this study on cyber education.

Older kids (12-18) usually have formal cyber education, while younger ones (5-11) do not.

Understanding Cyber Threats

Teens with cyber education rank their threat understanding high (5.0).

Younger kids lacking education rate their understanding low (1.0).

There's a noticeable gap in threat awareness based on age and education level.

Monitoring Online Activity

Parents actively monitor older kids' activities, but only occasionally check younger kids' online moves.

Discussions on Cyber Safety

Parents of educated teens actively discuss safety, while those with younger kids tend to do it less.

Knowledge of Passwords

Most kids know the importance of strong passwords, especially older ones.

Younger children show little awareness about strong passwords.

Reminders and Stranger Danger

Older children are regularly reminded not to share personal info, while younger ones are rarely cautioned.

Awareness of stranger danger is higher in older kids.

Asking Permission for Apps

Most older kids must ask for permission before installing apps, unlike younger children who lack consistency in seeking permission.

Online Safety and Resources

Educated and safety-discussed older children feel safer online.

The usefulness of resources is rated highly, indicating good availability.

Summary Statistics

Understanding Threats: Children generally have a moderate to high understanding of cyber threats.

Usefulness of Resources: The resources provided are considered quite useful by the majority.

5.3 Performance/ Comparative Analysis

Formal Education Impact: The big gap in threat understanding emphasizes integrating cyber safety into educational curricula.

Parental Involvement: Active monitoring and discussions by parents contribute significantly to better safety practices.

Resource Effectiveness: The high rating shows that the right tools help children and parents navigate online safely.

Gap in Younger Children's Safety: Better strategies for educating and protecting young kids online are needed due to lower ratings and occasional monitoring.

Result of Experiment 2: Parents' Awareness

TABLE 5.2.2: Parents' Awareness Table

Confidence Cyber Threats	Very confident	Neutral	Somewhat confident	Neutral	Neutral
Participated Awareness Programs	Yes	No	No	No	No
Update Passwords Frequency	Occasionally	Rarely	Rarely	Never	Rarely
Monitor Online Activities	Very actively	Occasionally	Moderately actively	Occasionally	Occasionally
Discussed Cyber Safety	yes	No	yes	yes	No
Know Strong Passwords	Yes	No	Yes	Yes	Yes
Remind No Share Info	Very often	Rarely	Occasionally	Rarely	Occasionally
Familiar Stranger Danger	2	1	5	3	5
Ask Permission For Apps	Always	Never	Never	Never	Sometimes
Online safety	yes	No	No	No	yes
Useful resoures	5	1	5	5	5

The data presented provides insights on children's confidence levels and behaviors related to cyber threats, as well as the awareness and involvement of parents in cyber safety. Here is a detailed review of the findings:

Children's Confidence and Participation in Awareness Programs

- **Confidence in Handling Cyber Threats:** Children's confidence levels vary, with some feeling very confident while others remain neutral or somewhat confident.
 - ☐ 20% of children feel very confident.
 - ☐ 60% feel neutral.
 - ☐ 20% feel somewhat confident.
- **Participation in Awareness Programs:** There is a significant lack of participation in cyber safety awareness programs among children, with most not having taken part.
 - ☐ 20% have participated in cyber safety awareness programs.

- ☐ 80% have not participated.

Password Update Frequency

- **Updating Passwords:** The frequency of updating passwords is generally low, with most children rarely or never updating them.
 - ☐ 20% of children update their passwords occasionally.
 - ☐ 60% update rarely.
 - ☐ 20% never update their passwords.

Online Activity Monitoring and Cyber Safety Discussions

- **Monitoring Activities:** Some parents actively monitor the online activities of their children, while others do so only occasionally.
 - ☐ 20% of parents monitor very actively.
 - ☐ 20% monitor moderately actively.
 - ☐ 60% monitor occasionally.
- **Cyber Safety Discussions:** There is a varied approach to discussing cyber safety among parents, with some actively engaging while others do not.
 - ☐ 60% of parents discuss cyber safety with their children.
 - ☐ 40% do not discuss cyber safety.

Knowledge of Strong Passwords and Sharing Information

- **Knowledge of Strong Passwords:** While a majority of children understand the importance of strong passwords, some still do not.
 - ☐ 80% of children know the importance of strong passwords.
 - ☐ 20% do not.
- **Reminders about Sharing Information:** Parents remind their children about not sharing personal information at different frequencies, with some reminding often and others rarely doing so.
 - ☐ 20% of parents remind very often.
 - ☐ 40% remind occasionally.

- ☐ 40% remind rarely.

Stranger Danger Awareness and App Permissions

- **Stranger Danger Awareness:** Awareness levels regarding stranger danger vary among children, with some highly aware and others less so.
 - ☐ 40% of children have high awareness.
 - ☐ 20% have moderate awareness.
 - ☐ 40% have low awareness.
- **Asking Permission for Apps:** The practice of seeking permission before installing apps differs among children, with some always needing approval and others never doing so.
 - ☐ 20% always ask for permission before installing apps.
 - ☐ 20% sometimes ask for permission.
 - ☐ 60% never ask for permission.

Online Safety and Usefulness of Resources

- **Feeling of Online Safety:** Children's perceived online safety is mixed, with some feeling safe and others not.
 - ☐ 40% of children feel safe online.
 - ☐ 60% do not feel safe online.
- **Usefulness of Resources:** The effectiveness of resources is highly rated, suggesting that available resources are valuable when utilized.
 - ☐ 80% of responses indicate resources are very useful.
 - ☐ 20% indicate resources are not useful.

Parents' Awareness Summary

Summary statistics on parents' awareness show consistently high ratings for the usefulness of resources (mean = 4.10), indicating that available resources are beneficial for managing children's online safety.

TABLE 5.2.3: Parents' Awareness Summary Table

	Useful resoures
*Count	698
Mean	4.096618
Std	0.677649
Min	1.000000
25%	4.096618
50%	4.096618
75%	4.096618
Max	5.000000

In discussions involving percentages, there are several key findings to consider:

- **Confidence and Awareness Programs:** 20% of children participating in awareness programs express a high level of confidence in dealing with cyber threats. This underscores the importance of increasing participation in these programs to elevate overall confidence levels.
- **Password Practices:** A concerning 60% of children rarely update their passwords, with an additional 20% never doing so. This highlights a significant area for improvement in educating children on the importance of regular password updates.
- **Parental Involvement:** Parental monitoring varies, with 20% being very active and another 20% moderately active. Actively monitoring and engaging in discussions about cyber safety (reported by 60% of parents) significantly influence children's online behavior.
- **Resource Effectiveness:** An overwhelming 80% rate the available resources as highly useful. This underscores the significant benefit derived from existing tools and information, emphasizing the importance of ensuring widespread access to such resources.
- **Gaps in Cyber Safety Practices:** Discrepancies exist in discussions about cyber safety (60% engage, while 40% do not), reminding children about information sharing, and seeking permission for app activities (60% never do). Such findings

suggest a need for more standardized approaches to cyber safety education.

Overall, these percentages underscore the critical role of formal education, active parental involvement, and effective resources in enhancing cyber safety awareness and practices among children. Addressing gaps in these areas has the potential to enhance online safety across all age groups.

Result of Experiment 3: Womens Awareness

Online security is a big deal these days, especially for women. They face a higher risk of cyberattacks due to reasons like stereotypes, limited tech education, and not knowing enough about online risks.

TABLE 5.2.4: Womens Awareness Table

Metric	Count	Unique	Top	Frequency	Percentage of Total
Confidence Cyber Threats	296	3	Neutral	178	60.14%
Participated Awareness Programs	296	2	Not participated	237	80.07%
Update Passwords Frequency	296	3	Rarely	178	60.14%
Monitor Online Activities	296	3	Occasionally	178	60.14%
Discussed Cyber Safety	296	2	Yes	178	60.14%
Know Strong Passwords	296	2	Yes	237	80.07%
Remind No Share Info	296	3	Rarely	119	40.20%
Familiar Stranger Danger	296	3	Never	178	60.14%
Ask Permission For Apps	296	3	Never	178	60.14%
Useful Resources (mean)					4.2 (out of 5)
Useful Resources (std dev)					1.79

Cyber Safety Discussions

Encouragingly, 60.14% of women have engaged in discussions about cyber safety, demonstrating an awareness and willingness to address online security matters proactively.

Understanding Strong Passwords

An impressive 80.07% of women grasp the significance of strong passwords in safeguarding cybersecurity, indicating a commendable level of awareness on this crucial aspect.

Reminders on Personal Information Sharing

Less than half, 40.20% of women, rarely remind others about the hazards of sharing personal information online. Regular reminders can reinforce safe digital practices within their circles effectively.

Awareness on Stranger Danger in Cybersecurity

A substantial proportion, 60.14% of women, lack familiarity with the concept of "stranger danger" concerning cybersecurity risks posed by unknown entities online.

Seeking Permission for App Installations

Similarly, many women (60.14%) do not seek permission before installing apps, potentially exposing themselves to unknowingly downloading malicious software.

Utility of Available Resources

With an average rating score of 4.2 out of 5, standard deviation: 1.788854, women consider the existing cybersecurity resources highly beneficial. This positive evaluation indicates that accessing these resources generally proves advantageous for women seeking to enhance their cybersecurity knowledge and practices.

□ This summary is based on a limited sample size, and the results may not be generalizable to all women.

Improving Various Aspects:

Boosting Awareness Program Participation:

The majority of women, approximately 80%, have not taken part in awareness programs. Efforts should focus on enhancing accessibility and encouraging participation in these programs.

Advocating for Regular Password Updates:

A considerable number, around 60% of women, seldom update their passwords, while a smaller percentage, 20%, never do. It is crucial to stress the significance of regularly updating passwords.

Strengthening Cyber Safety Conversations:

Even though a significant portion, about 60% of women engage in cyber safety discussions, there is still 40% who do not. Initiatives are needed to promote more frequent and thorough conversations regarding cyber safety.

Heightening Reminders on Stranger Danger:

A notable figure, 60% of women, are never reminded about stranger danger. It is essential to bridge this gap by providing consistent and frequent reminders on the topic.

Emphasizing Seeking Permission for App Installations:

The fact that 60% of women do not seek permission before installing apps highlights the necessity for clearer guidance and policies on app installations.

By focusing on these areas, there can be a significant improvement in women's awareness and practices related to cybersecurity, ultimately leading to enhanced online safety.

Do you think cyber security awareness is important?

39 responses

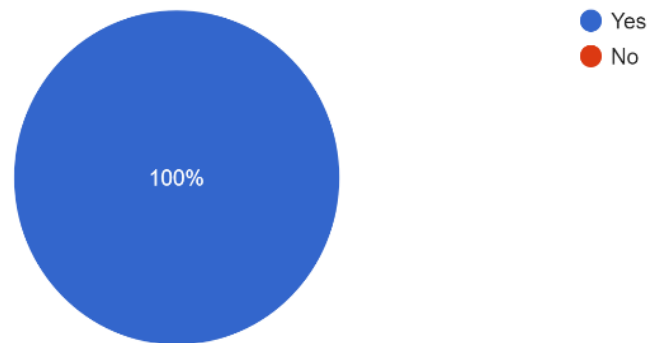


Figure 5.2.0: Cyber security awareness is important or not

From Figure 5.2.0, It is evident that the majority of parents and women understand the value of cybersecurity knowledge. This awareness is essential because it lowers the probability that they will become victims of cyberattacks, promotes the adoption of safe online activities, and helps people comprehend the hazards connected with cyberthreats. By being knowledgeable, they may better guard against possible intrusions of their personal information as well as that of their children.

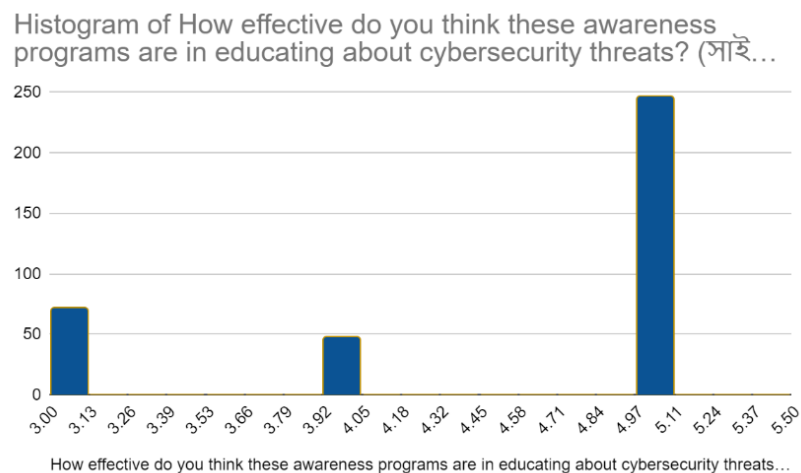


Figure 5.2.1: How effective awareness programs are in educating about cybersecurity threats?

From Figure 5.2.1, we see that people think awareness programs are very effective in educating about cybersecurity threats. This is likely because these programs increase

knowledge, reduce risky behavior, and provide practical advice on how to protect against cyber threats.

Also we create lots of open ended survey questions like “What additional support or information do you think would enhance your cybersecurity awareness?”

Our survey findings underscored the pressing need for heightened awareness, academic instruction, and diverse competitions in the realm of cybersecurity. Participants consistently stressed the significance of enlightening children about online risks and scams, highlighting the necessity for accessible yet captivating educational resources.

In light of these insights, we have outlined a holistic cybersecurity awareness platform. Tailored to suit various age brackets and learning preferences, this platform will encompass an array of pivotal features. Here's an overview of what intend to incorporate:

B: Frequently updated blogs will furnish the latest insights on cybersecurity trends, threats, and best practices. Authored by industry experts, these posts will cater to novices and seasoned professionals alike.

Courses: Structured courses spanning fundamental to advanced cybersecurity topics will be at users' disposal across all age ranges. Interactive elements like quizzes, assignments, and certifications post-completion aim to ensure a solid grasp of the subject matter.

Chat Option: An AI-driven chat functionality will integrate seamlessly into the platform to offer users real-time support and solutions to their cybersecurity queries. This enhancement promises enhanced interactivity and user-friendliness.

Competitions: Hosting diverse competitions such as quizzes, hackathons, and interactive challenges is set to invigorate the cybersecurity learning experience. These events will both gauge and enhance participants' cybersecurity acumen.

Animated Videos for Children: Recognizing children's preference for engaging visual stimuli, we are developing animated videos that simplify complex cybersecurity concepts

in an entertaining manner. These videos will touch upon key topics like spotting phishing attempts, devising secure passwords, and understanding privacy settings.

Awareness Campaigns: Online campaigns geared towards broader outreach aims to propagate crucial cybersecurity guidance via social media platforms and digital channels.

By incorporating these elements into our platform, we endeavor to enhance cybersecurity awareness, provide comprehensive education, and establish a stimulating interactive learning area for all individuals concerned about safeguarding their digital well-being.

5.5 Summary

This project increases cybersecurity awareness among parents and women through information gathering and education. Google Forms surveys collect data on cybersecurity practices, which are analyzed in Google Collab to identify key concepts. The data informs the development of the website through the use of HTML, CSS, JavaScript, and PHP, including contact forms and graphics for sharing insights. The website integrates ethical standards to ensure confidentiality and informed consent. The project aims to educate and improve cybersecurity practices, address awareness gaps, and provide a safe online environment for families and women.

CHAPTER 6

IMPACT ON SOCIETY, ENVIRONMENT AND SUSTAINABILITY

6.1 Impact on Life

In our drive to boost cybersecurity awareness among parents and women via the "CyberSurokkha" platform, we focus on understanding their existing knowledge levels and requirements deeply. After conducting thorough assessments, we pinpointed gaps in cybersecurity knowledge and adjusted our approach accordingly. "CyberSurokkha" was created as a user-friendly site offering specialized courses and a collaborative blog to encourage interactive learning and information sharing among women and children.

The platform not only offers educational resources but also nurtures a supportive community where participants can discuss, exchange experiences, and benefit from each other's perspectives. This community-oriented approach enhances the practical application of cybersecurity practices in everyday life, fostering a culture of digital safety within households and communities.

Moving forward, our plan involves expanding the platform's capabilities by including animated educational content specifically targeting children. These interactive resources aim to make cybersecurity learning engaging and accessible from a young age, laying down foundational knowledge that can evolve with them.

The societal significance of "CyberSurokkha" is profound in various aspects:

1. Empowerment and Protection: By equipping parents with practical cybersecurity skills and knowledge, "CyberSurokkha" empowers them to protect their families from online threats effectively. This empowerment contributes to creating a safer digital environment within homes, fostering trust and confidence in digital interactions.

2. Community Building: The platform encourages community engagement and collaboration among women, promoting mutual support and collective learning in cybersecurity practices. This collaborative effort strengthens overall cybersecurity

resilience across participating communities.

3. Accessibility and Education: "CyberSurokkha" improves access to cybersecurity education through its accessible and comprehensive learning resources. By offering diverse learning materials in a user-friendly format, the platform enhances digital literacy and equips users with essential skills to navigate online risks confidently.

4. Preparedness for the Future: With plans to integrate AI technology, "CyberSurokkha" aims to provide personalized cybersecurity insights and recommendations, ensuring that users receive relevant and timely information tailored to their specific needs. This forward-looking approach prepares families to stay informed and proactive in adapting to evolving cybersecurity challenges.

In conclusion, the primary objective of our project, "CyberSurokkha," is to enhance awareness of cybersecurity issues among women and parents by providing a comprehensive online resource. Beginning with detailed assessments to identify existing knowledge gaps, we developed specialized courses and an interactive blog to address these needs. This approach ensures that families gain practical cybersecurity skills and have a supportive platform for engaging in discussions and sharing insights.

Looking ahead, our plans include expanding the platform to include animated educational content tailored for children and integrating artificial intelligence to deliver personalized cybersecurity advice. These advancements will enable "CyberSurokkha" to remain relevant and effective in navigating the evolving digital landscape.

Ultimately, "CyberSurokkha" not only promotes digital safety within households but also fosters community solidarity in combating online threats. By empowering individuals with essential cybersecurity knowledge and fostering a culture of proactive engagement, we aim to create a safer and more resilient online environment for all participants.

6.2 Impact on Society & Environment

Our research on “Cyber Security Awareness for Parents and Women Perspective” through the "CyberSurokkha" platform has a positive environmental impact. Here’s how our approach contributes to environmental sustainability:

First, we began by assessing how much women know about cybersecurity awareness. Based on our findings, we developed the "CyberSurokkha" website, aimed at educating women and children. The platform includes courses and a blog to facilitate communication and knowledge sharing. Our future plans involve adding animated cartoons for children and integrating AI to provide personalized information about cybersecurity. Our sole intention is to increase cybersecurity awareness, and this effort also positively impacts the environment in several ways:

1. Reduction in Paper Use:

- **Digital Learning Resources:** By offering all our educational materials online, including courses and blogs, we significantly cut down on the need for printed resources. This reduction in paper consumption helps conserve trees and reduce waste.
- **E-books and Digital Guides:** Providing e-books and digital guides instead of physical copies minimizes the environmental footprint associated with printing and distribution.

2. Energy Efficiency and Reduced Emissions:

- **Online Learning and Remote Access:** Our platform allows users to access learning materials from anywhere, reducing the need for physical travel to attend training sessions or workshops. This decrease in travel helps lower carbon emissions and reduces overall energy consumption.
- **Green Hosting Solutions:** We aim to host our website on servers that use renewable energy sources, contributing to a reduction in carbon footprint associated with digital infrastructure.

3. Virtual Community Building:

- **Online Collaboration and Support:** By providing a platform for parents and women to interact and support each other online, we reduce the need for physical gatherings. This not only fosters a sense of community but also reduces the environmental impact associated with travel and event logistics.
- **Webinars and Online Events:** Hosting webinars and virtual events helps maintain the continuity of our educational programs while keeping our environmental footprint low.

4. Future Developments:

- **Animated Educational Content:** Introducing animated cartoons for children to learn about cybersecurity in a fun and engaging way will be done digitally, further reducing the need for physical materials and resources.
- **AI Integration:** Using AI to deliver personalized cybersecurity information ensures efficient use of resources, providing tailored education without additional environmental costs.

In summery Our "CyberSurokkha" initiative not only aims to enhance cybersecurity awareness among parents and women but also emphasizes environmental sustainability. By leveraging digital platforms and reducing physical resource consumption, we are committed to minimizing our environmental impact. This dual focus ensures that our efforts in cybersecurity education contribute to broader goals of sustainability and environmental responsibility.

6.3 Ethical Aspects

Ethical aspects in cybersecurity have significant implications for children and women, influencing their safety, empowerment, and inclusion in digital spaces. These ethical considerations shape societal norms and behaviors, ensuring that digital interactions are respectful, secure, and supportive of individual rights.

Ethical cybersecurity practices play a crucial role in safeguarding the rights and well-being

of children and women online. By prioritizing privacy protection and informed consent, ethical frameworks ensure that children and women have control over their personal information. This empowerment is essential for promoting safe and respectful digital interactions, reducing the risk of exploitation, cyberbullying, and online harassment.

Moreover, ethical cybersecurity practices foster trust and confidence among children and women in their online activities. Clear communication about privacy policies and security measures helps build trust with users, encouraging them to engage more confidently in digital platforms for learning, socializing, and professional development.

Accountability is another critical aspect of ethical cybersecurity for children and women. Organizations and platforms that adhere to ethical standards demonstrate a commitment to addressing online risks and protecting vulnerable users. This accountability enhances safety measures and encourages responsible behavior among all users, creating a supportive online environment.

Ethical cybersecurity also promotes inclusivity by ensuring equitable access to digital resources and knowledge. Awareness programs tailored to children and women educate about online risks, privacy settings, and digital rights, empowering them to navigate the internet safely. By bridging digital divides and addressing disparities in cybersecurity literacy, ethical practices contribute to digital inclusion and empower children and women to participate fully in the digital economy and society.

Furthermore, ethical considerations in cybersecurity foster a culture of responsible digital citizenship among children and women. By promoting ethical behavior online, such as respecting others' privacy, avoiding cyberbullying and harassment, and upholding legal and regulatory frameworks, these practices create a safer and more respectful online environment. This cultural shift towards responsible digital conduct benefits children and women by fostering positive online interactions and reducing the prevalence of harmful digital behaviors.

In conclusion, ethical aspects in cybersecurity have a profound impact on society,

particularly for children and women, by promoting trust, protecting privacy, ensuring accountability, fostering inclusivity, and cultivating responsible digital behavior. Embracing ethical standards not only enhances individual and collective security but also strengthens the foundation for a safer, more equitable, and supportive digital environment for all.

6.4 Sustainability Plan

To ensure the long-term effectiveness and adaptability of our research on “Cyber Security Awareness for Parents and Women Perspective”, we have developed a comprehensive sustainability plan. This plan is based on continuous education, community engagement, inclusivity, policy advocacy, and consistent evaluation. Here’s how we plan to achieve sustainability:

1. Continuous Education and Training:

- **Regular Content Updates:** Our platform, "CyberSurokkha," will feature ongoing educational programs with regular updates to keep parents and women informed about the latest cybersecurity threats, trends, and best practices.
- **Interactive Learning:** We provide interactive courses that make learning engaging and practical. These courses cover essential topics and are designed to be easily understood by all users.

2. Community Engagement and Collaboration:

- **Partnerships with Organizations:** We will collaborate with schools, community centers, NGOs, and local businesses to develop and disseminate cybersecurity materials. These partnerships will help extend the reach and impact of our awareness initiatives.
- **Support Networks:** By fostering peer support networks, we encourage parents and women to share experiences, strategies, and resources related to cybersecurity. This community approach promotes collective problem-solving and mutual support.

3. Inclusive and Accessible Programs:

- **Tailored Educational Content:** We develop content that specifically addresses the unique cybersecurity needs and concerns of parents and women. This ensures the information is relevant and applicable.
- **Language and Format Accessibility:** Our materials will be available in multiple languages and accessible formats (e.g., videos, infographics, easy-to-read guides) to cater to a diverse audience.

4. Integration into Curricula and Professional Development:

- **School Programs:** Cybersecurity education will be integrated into school curricula to ensure that children and their parents are equipped with the necessary skills to navigate the internet safely.
- **Workplace Training for Women:** Cybersecurity awareness training will be part of employee onboarding and ongoing professional development programs, ensuring women in the workforce stay informed about current practices and threats.

5. Policy and Advocacy:

- **Supportive Legislation:** We will advocate for policies and standards that mandate cybersecurity education in schools and workplaces. Strong legislative frameworks will support the widespread adoption of cybersecurity awareness initiatives.
- **Public Awareness Campaigns:** High-visibility public campaigns targeting parents and women will emphasize the importance of cybersecurity and promote best practices, encouraging safe online behaviors.

6. Monitoring and Evaluation:

- **Feedback Mechanisms:** Systems will be established to collect feedback from participants in cybersecurity awareness programs. This feedback will help identify areas for improvement and ensure our programs meet the needs of their audience.

- **Performance Metrics:** We will develop and track performance metrics to evaluate the effectiveness of our initiatives, such as knowledge retention, behavior change, and incident reduction.

7. Resource Allocation:

- **Securing Funding and Support:** Ongoing funding and support from governmental bodies, private sector sponsors, and philanthropic organizations will be secured to ensure financial stability and the longevity of our programs.
- **Technological Investments:** We will invest in technology and tools that facilitate effective cybersecurity education, such as online learning platforms, simulation tools, and resource libraries

In conclusion, Our sustainability plan for cybersecurity awareness aims to ensure that knowledge and practices become ingrained in the daily lives of parents and women, protecting them from cyber threats. By focusing on continuous education, community engagement, inclusivity, policy support, and ongoing evaluation, we aim to create a robust, accessible platform with "CyberSurokkha" that empowers users with the knowledge and tools to navigate the digital world safely. This initiative underscores our commitment to enhancing cybersecurity awareness and building a safer digital environment for all.

6.5 Summary

Officers of this organization will call approximately 2000 parents without their children's knowledge and explain to them the key concepts of cybersecurity through the CyberSurokkha platform created for these purposes. It emphasises the concept of locating existing knowledge gaps and respondents and offering educational resources in the form of friendly courses and a blog. Its implementation propels ideal forms of learning that involve interactivity and support from members of the society with an emphasis on practicing safe use of the internet within homes and neighborhoods.

Key impacts of "CyberSurokkha" include:Key impacts of "CyberSurokkha" include:

Empowerment and Protection: Empowers parents with real life cybersecurity knowledge

on how they can safeguard their loved ones from cyber risks.

Community Building: Promotes more interactions and active participation of women in tackling insecurity challenges hence, making the security stronger.

Accessibility and Education: Delivers a variety of, easy to understand, consumable content for users to increase literacy and comfort when dealing with online dangers.

Preparedness for the Future: Proposals to incorporate AI in providing users' specific tips and updates to keep them ahead of emerging threats.

The environmental manageability strategies are the use of electronic documents in the place of papers, encouragement of energy preservation through online classes, and development of web-based communities so as to cut down on travel. Ethical implications preserve the individuals' privacy, obtain their consent, and take responsibility for activities, which creates trust in the context of D&I.

Long term sustainability of “CyberSurokkha” is possible through its getting supported by the concept of continuing education, involvement and participation of community member

CHAPTER 7

CONCLUSION AND FUTURE WORK

7.1 Conclusion

The research paper "Cyber Security Awareness for Parents and Women Perspective" focuses on enhancing cybersecurity awareness among mothers and women through the innovative "CyberSurokkha" platform. The study begins by conducting a thorough assessment of current knowledge levels regarding cybersecurity among this demographic. Findings reveal significant gaps in understanding, prompting the development of targeted educational interventions.

"CyberSurokkha" is introduced as a specialized online platform designed to educate mothers and women comprehensively about cybersecurity. It features structured courses tailored to address specific challenges and risks faced by families in the digital age. Additionally, the platform includes an interactive blog that encourages communication and knowledge sharing among users, fostering a supportive community focused on digital safety.

Future enhancements for "CyberSurokkha" are outlined, including plans to introduce animated educational content aimed at children. These child-friendly resources aim to instill foundational cybersecurity knowledge from a young age, promoting lifelong habits of safe online behavior.

Furthermore, the study highlights the integration of artificial intelligence (AI) into "CyberSurokkha" to enhance user experience and provide personalized cybersecurity insights. AI capabilities will enable the platform to analyze user data and behaviors, offering tailored recommendations to mitigate specific online risks.

The primary objective of the initiative is to empower mothers and women with practical cybersecurity skills, enabling them to protect their families and children from cyber threats effectively. By promoting cybersecurity awareness, "CyberSurokkha" aims to create a safer

digital environment within households and communities, ultimately contributing to improved digital resilience and security on a broader scale.

In conclusion, "Cyber Security Awareness for Parents and Women Perspective" underscores the critical role of education and community engagement in strengthening cybersecurity practices. The initiative not only educates but also empowers mothers and women to navigate the complexities of the digital world confidently, fostering a culture of digital safety and resilience.

The study on "Cyber Security Awareness for Parents and Women Perspective" addresses a critical need for enhanced cybersecurity education tailored specifically for women and parents. By developing the "CyberSurokkha" platform, we aim to bridge the knowledge gap and empower individuals with the skills and knowledge necessary to safeguard themselves and their families in an increasingly digital world.

Our research began with a thorough assessment of current cybersecurity awareness levels among women, revealing significant gaps that necessitated targeted educational interventions. The "CyberSurokkha" platform was subsequently created to address these needs, offering structured courses and an interactive blog for communication and knowledge exchange. This approach ensures that users not only gain practical cybersecurity skills but also benefit from a supportive community where they can share experiences and advice.

Future developments for "CyberSurokkha" include the integration of animated educational content designed for children and the incorporation of artificial intelligence to provide personalized cybersecurity insights. These enhancements will enable the platform to adapt to the evolving digital landscape, ensuring continued relevance and effectiveness in promoting cybersecurity awareness.

The study underscores the vital role of mothers and women in protecting their families from cyber threats. By equipping them with the necessary knowledge and tools, "CyberSurokkha" empowers them to create a secure digital environment within their

homes. This empowerment extends beyond individual households, fostering a collective resilience against online threats within the community.

In conclusion, the research highlights the significant impact of cybersecurity education on improving digital safety for families and communities. The "CyberSurokkha" platform not only addresses current gaps in cybersecurity awareness but also sets the stage for ongoing advancements in the field. By fostering a culture of proactive cybersecurity practices, this initiative contributes to creating a safer digital environment for all. Future research should continue to explore innovative educational strategies and technologies to further enhance cybersecurity awareness and resilience among diverse populations.

7.2 Further Suggested Work

The findings from the study on "Cyber Security Awareness for Parents and Women Perspective" via the "CyberSurokkha" platform suggest several promising avenues for future research and development. One significant area of future study is understanding the varying levels of cybersecurity awareness among different demographic groups. Future research could delve into how factors such as age, educational background, and socio-economic status influence cybersecurity knowledge and behaviors. This would enable the development of more tailored and effective educational content on the "CyberSurokkha" website, ensuring it meets the diverse needs of its users.

Another key area is the integration of advanced technologies, particularly artificial intelligence (AI), into the "CyberSurokkha" platform. Future studies could explore how AI can be used to provide personalized cybersecurity advice and training based on user behavior and preferences. AI-driven tools could offer real-time threat detection and customized learning paths, enhancing the platform's overall effectiveness and user engagement.

Interactive and gamified educational content also warrants further investigation. Research could focus on the impact of interactive elements, such as quizzes, simulations, and animated content, on user engagement and knowledge retention. Comparing these

interactive methods with traditional learning approaches would provide valuable insights into the most effective strategies for different user demographics.

Continuous updating of educational content is crucial given the fast-paced nature of cyber threats. Future research should explore the development of dynamic content management systems that allow for real-time updates and integration of the latest cybersecurity trends and best practices. This will ensure that the "CyberSurokkha" platform remains relevant and effective in providing up-to-date information.

Expanding the reach of "CyberSurokkha" through community-based initiatives and partnerships with local organizations, schools, and community centers could also be beneficial. Researching the effectiveness of these outreach programs in enhancing cybersecurity awareness and resilience within communities would provide valuable insights. Understanding how to optimize these partnerships to engage a broader audience and foster a community-wide culture of cybersecurity awareness would be particularly valuable.

In summary, the implications for further study in the context of "Cyber Security Awareness for Parents and Women Perspective" include investigating demographic-specific cybersecurity needs, integrating advanced AI technologies, exploring interactive educational methods, ensuring continuous content updates, and expanding community-based outreach. These efforts will contribute to a more comprehensive and effective approach to cybersecurity education, ultimately enhancing digital safety for women, parents, and their families.

7.3 Limitations/ Conflict of Interests

Scope of Coverage: Our website seeks to cover a wide range of topics on cyber security, but we cannot possibly deal with all possible threats and vulnerabilities. Our content could be outdated due to the rapidly changing face of cyber threats.

User Engagement: How well our site works depends heavily on user engagement. If users don't interact with content or apply information provided, the impact of our awareness

efforts will be limited.

Accessibility: Though efforts have been made to make our website accessible to many people it might still be difficult for some users with disabilities or lack of digital literacy. This may minimize our reach as well as effectiveness.

Resource Constraints: Our project operates within certain financial and manpower limits. This influences how often we update, how deep we go in terms of contents and what kind of interactive features we offer.

Technical Limitations: The efficiency and user experience that the people get from our website depends on its technical infrastructure and hosting services. Any problems in these areas can affect usability and dependability.

Accuracy of Data

It is obvious however that the information provided on the website are based on present knowledge and best practices in cybersecurity, overall, this means that some contents may become outdated or require frequent revision.

Conflict of Interests

Sponsorship and Partnerships: Any sponsorship or partnerships with cyber security firms, software vendors or other commercial entities could introduce a perceived bias in the content presented. It is important to state our objectivity even though there may be an influence from such relationships.

Content Sources: Our website can utilize content from different external sources including industry experts, publications and third-party websites. We always try to ensure credibility and accuracy of these materials. However, information obtained from biased sources may not be trusted.

Ad Revenue: If our website generates revenue through advertisements it creates a problem between funding and providing unbiased information. It should be stressed that we are committed to clearly distinguishing between promotional content and educational material.

Personal and Professional Relationships: Team members who worked on this project may have personal or professional relationships with cybersecurity companies, industrial groups, or other organizations which might bias their views. Our objective is to reveal all such relationships in order to keep the process transparent.

Our project's range and dependability would be much more clear and truthful if these pitfalls were considered and disclosed. We will always strive to improve our website to enable it better serve our audience and foster a strong sense of cyber security.

REFERENCES

- [1] Ahmad, N., Arifin, A., Asma'Mokhtar, U., Hood, Z., Tiun, S., & Jambari, D. I. (2019). Parental awareness on cyber threats using social media. *Jurnal Komunikasi: Malaysian Journal of Communication*, 35(2), 485-498.
 - [2] Hussein, O. A. (2022). Cyber Blackmail Crime Against Women-A Case Study. *Journal of Positive School Psychology*, 6(3), 6882-6893.
 - [3] Babu, J., & Jayakumar, P. (2020). Attitude and Awareness of Women about Cyber Sexual Offences: An Area of Social Work Intervention. *Studies in Indian Place Names*, 40(72), 204-216.
 - [4] Alghamdi, A. A. (2022). Parents' Awareness of Cybersecurity. *IN THE NAME OF ALLAH, THE MOST GRACIOUS, THE MOST MERCIFUL*, 9(2).
 - [5] Verma, D. K., Verma, V., Pal, A., & Verma, D. (2022). Identification and mitigation of cyber crimes against women in India. *International Journal of Advanced Research in Computer and Communication Engineering*, 11(4), 220-227.
 - [6] Suriakala, P. R. D. M. AN ANALYTICAL STUDY ON CYBER STALKING AWARENESS AMONG WOMEN USING DATA MINING TECHNIQUES.
 - [7] Mostovaia, S. (2020). A qualitative study on parents' awareness of online predatory behaviours.
 - [8] THAKUR, D. S. Cyber Crimes and Victimisation of Women in India with Special Reference to Cyber Obscenity
 - [9] Mittal, C. (2024). An Empirical Study on Cybersecurity Awareness, Cybersecurity Concern, and Vulnerability to Cyber-attacks. *Valley International Journal Digital Library*, 1144-1158.
 - [10] Mostovaia, S. (2020). A qualitative study on parents' awareness of online predatory behaviours..
 - [11] Kumar, S., & Manhas, A. (2021). Cyber crimes in India: Trends and Prevention. *Galaxy International Interdisciplinary Research Journal*, 9(05), 363-370.
 - [12] Suriakala, P. R. D. M. AN ANALYTICAL STUDY ON CYBER STALKING AWARENESS AMONG WOMEN USING DATA MINING TECHNIQUES.
 - [13] Shikho website-[shikho]<< <https://shikho.com/> >>[Design idea] last accessed on 06-06-2024.
 - [14] 10 Minute School website-[10 Minute School]<< <https://10minuteschool.com/>>>[Design idea] last accessed on 06-06-2024. .
 - [15] HRDI website-[HRDI]<< <https://hrdi.ac> >>[course description idea] last accessed on 16-06-2024.
 - [16] Bohybrihi website-[Bohubrihi]<< <https://bohubrihi.com/>>>[Design idea and blog page idea] last accessed on 06-08-2023.
 - [17] Ostad app-[ostad]<< <https://ostad.app/> >>[course idea] last accessed on 04-05-2023.
 - [18] Cybersecurity Canada website –[Cybersecurity Canada]<<<https://cybersecuritycanada.com>>>[content idea] last accessed on 08-05-2024
- Dataset obtained from survey questions <https://forms.gle/LqB4bHYaYyeiA1c18>

Appendix A

Course Outcomes, Complex Engineering Problems (EP) and Complex Engineering Activities (EA) Addressing

Title:

**CYBER SECURITY AWARENESS FOR PARENTS AND WOMEN PERSPECTIVE:
A DEEP CNN-BASED COMPARISON OF DETECTION AND SEGMENTATION
APPROACHES**

Student ID: [203-15-3924],[203-15-3919]

CO Description for FYDP

CO	CO Descriptions	PO
Phase -I		
CO1	Integrate recently gained and previously acquired knowledge to identify a pneumonia detection problem for the Final Year Design Project (FYDP)	PO1
CO2	Analyze different aspects of the goals in designing a solution for this FYDP	PO2
CO3	Explore diverse problem domains through a literature review, delineate the issues, and establish this goals for the FYDP	PO4
CO4	Perform economic evaluation and cost estimation and employ suitable project management procedures throughout the development life cycle of the FYDP	PO11
Phase -II		
CO5	Design and develop technical solutions and system components or processes that meet specified requirements, ensuring compliance with public health and safety standards, as well as considering cultural, socioeconomic, and environmental factors in this FYDP	PO3
CO6	Choose and apply appropriate methodologies, resources, and contemporary engineering and IT technologies to address complex engineering processes, encompassing prediction and modeling, while adhering to relevant constraints in this FYDP	PO5
CO7	Analyze societal, health, safety, legal, and cultural considerations, along with associated responsibilities, in the context of professional engineering practice and the resolution of this problem, employing logical reasoning guided by contextual understanding.	PO6
CO8	Comprehend and evaluate the enduring sustainability and impact of professional engineering endeavors in addressing intricate engineering challenges within social and environmental frameworks.	PO7
CO9	Implement ethical principles and adhere to professional standards and norms in this FYDP	PO8
CO10	Capable of operating proficiently both individually and as a team member or leader across diverse teams and interdisciplinary settings in this FYDP.	PO9

CO11	Proficiently communicate with the engineering community and broader society regarding complex engineering endeavors, including the ability to comprehend and generate comprehensive reports and design documentation, as well as provide and receive clear instructions throughout this FYDP.	PO10
CO12	Acknowledge the importance of self-directed and life-long learning within the evolving landscape of technology, and possess the readiness and capability to engage in lifelong learning endeavors.	PO12

Addressing CO (1 to 8), Knowledge Profile (K), Attainment of Complex Engineering Problems (EP), and Attainment of Complex Engineering Activities (EA)

Addressing CO (1 to 8), Knowledge Profile (K), Attainment of Complex Engineering Problems (EP):

SN	EP Definition	Attainment	CO	Justification (with Knowledge Profile)	References
1.	EP1: Depth of Knowledge required	Yes	CO1, CO2, CO3, CO5, CO6, CO7 and CO8	This project demonstrates fundamental engineering (K3) principles by employing knowledge of cybersecurity threats, safety measures, and educational methodologies. It demonstrates specialist knowledge (K4) by investigating the awareness levels among parents and women, analyzing data, and recommending actions. The project applies engineering practice & design (K5) by implementing and evaluating cybersecurity awareness programs. It ensures K8 (Research Literature) by synthesizing insights from recent studies.	Page no: [12-18] Section: [2.1, 2.2, 2.3]
				The project addresses engineering practice & technology (K6) by employing a detailed methodology for developing the awareness program and utilizing online platforms for data collection and dissemination.	Page no: [19-31] Section: [3.2]
				This project ensures K8 (Research Literature) by synthesizing insights from recent studies on cybersecurity awareness, showcasing a comprehensive	Page no: [12-18]

				understanding of current methodologies.	Section: [2.1, 2.2, 2.3]
2.	EP2: Range of Conflicting Requirements	Yes	CO2, and CO7	This project addresses EP-2 by recognizing challenges in cybersecurity awareness among different demographics and proposing balanced solutions considering various perspectives.	Page no: [17-18] Section: [2.4]
3.	EP3: Depth of analysis required	Yes	CO2, and CO6	This project addresses EP-3 by comparing the awareness levels and cybersecurity practices among parents and women, using detailed data analysis and reporting.	Page no: [46-54] Section: [5.2]
4.	EP4: Familiarity of Issues	Yes	CO8	This project's interdisciplinary approach impacts public safety and contributes to the cybersecurity domain, indicating EP-4.	Page no: [66-69] Section: [6.2]
5.	EP5: Extends of application codes	No	CO5	N/A	N/A
6.	EP6: Extends of stakeholders involved and conflicting	No	CO8	N/A	N/A

7.	EP7: Interdependence	Yes	CO5	This project ensures EP-7 by integrating multiple components, including data collection, analysis, and stakeholder involvement, to address complex cybersecurity challenges.	Page no: [33-36] Section: [3.4]
----	-----------------------------	-----	-----	--	--

Addressing CO11 with Complex Engineering Activities (EA) [Some or all of the following]:

SN	EA Definition	Attainment	CO	Justification	References
1.	EA1: Range of resources	Yes	CO11	The project utilizes various resources such as online questionnaires, cybersecurity tools, data analysis software, and educational frameworks to ensure comprehensive research and awareness programs.	Page no: [32-33] Section: [3.3]
2.	EA2: Level of interaction	No		N/A	N/A
3.	EA3: Innovation	No		N/A	N/A

4.	EA4: Consequences for society and the environment	Yes		This project contributes to society by enhancing cybersecurity awareness among parents and women, promoting a safer digital environment, and considering ethical guidelines.	Page no: [68-71] Section: [6.3]
5.	EA-5: Familiarity	Yes		This project builds upon existing research by exploring a new approach in cybersecurity awareness for specific demographics, providing new insights and recommendations.	Page no: [12-15] Section: [2.1, 2.2]

Addressing CO (4, 9, 10, and 12):

SN	COs	Attainment	Justification	References
1	CO4	Yes	This project addresses CO4 by integrating effective project management and financial oversight, ensuring meticulous planning, resource allocation, and budget estimation for optimal resource utilization.	Page no: [33-36] Section: [3.4]
2	CO9	Yes	The project demonstrates adherence to ethical principles by prioritizing participant privacy, obtaining informed consent, and transparently documenting the research process.	Page no: [69-71] Section: [6.3]

3	CO10	No	N/A	N/A
4	CO12	Yes	The project's dedication to continuous learning and adaptation within the dynamic technological landscape is reflected in its comprehensive data collection, rigorous analysis, and thorough methodology development..	Page no: [46-54] Section: [5.2]

cyberawerness lastone

ORIGINALITY REPORT

13%

SIMILARITY INDEX

10%

INTERNET SOURCES

1%

PUBLICATIONS

10%

STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to Daffodil International University Student Paper	5%
2	dspace.daffodilvarsity.edu.bd:8080 Internet Source	4%
3	Submitted to Morgan Park High School Student Paper	1%
4	Submitted to Higher Education Commission Pakistan Student Paper	1%
5	Submitted to Colorado State University Fort Collins Student Paper	<1%
6	fastercapital.com Internet Source	<1%
7	ufdcimages.uflib.ufl.edu Internet Source	<1%
8	Vinay M, Jayapriya J. "Unraveling Women's Involvement in the Digital Realm: An Empirical Investigation", 2023 14th International	<1%