Project Reflection

Generative AI: Navigating Short-term Skepticism and Long-term Promises

A logo with text on it

Description automatically generated

Unit: COIT20265: Networks and Information Security Project

Student Name: Bhuwan Thapa (12196590)

Project Mentor: Dr Ahmedi Azra

Date: 30/09/2024

CQUniversity Australia

Table of Contents

[Task Completed 3](#_Toc178434749)

[Newly Developed Skills 4](#_Toc178434750)

[Application of Existing Skills 5](#_Toc178434751)

[Contribution of Team Members 6](#_Toc178434752)

[Reflection on Project Experience 6](#_Toc178434753)

[Portfolio Contribution 7](#_Toc178434754)

# Task Completed

Here, I have listed the task that I completed individually while completing the group project.

|  |  |  |
| --- | --- | --- |
| **Task** | **Description** | **Deliverables** |
| Introduction of the project and project planning. | In this part I have described about the details introduction of the project that includes project aim, project planning and the results that we suppose to deliver at the end of the project. | This task delivers that complete understanding of the project, project plan and provide the road map for future planning. |
| Problems from business and technical perspective for using GenAI like ChatGPT and Gemini. | This task describes the issues arises due to the implementations of GenAI in terms of business and technical perspective. The problems due to this reason includes intellectual property concerns, economic disruption, managing expectations, ethical implementations, data quality and bias, technical expertise and collaboration etc. | This task figures out to differentiate complete picture of pros an cons GenAI in general terms. |
| Cybersecurity related issues and mitigation plan with the implementation of GenAI. | Here, I have described about the cybersecurity related issues such as data protection and privacy, web application security, social engineering attacks, phishing attacks etc and also provided the mitigation plan with implementation of GenAI such as password protection, vulnerability scanning and filtering, threats hunting queries and uses of security protection layers etc. | This task provides the understanding of importance of using GenAI for reducing cybersecurity issues. |
| Disaster recovery and business continuity plan for project management. | This task is for the plan to recover from the major disruption during the project progress. The disruption could be cyber-attacks, data loss, human errors, hardware and software failures etc. | This plan provides how to overcomes, prevent harm and damages from disastrous issues and continue the project implementations. |
| Industry analysis, stakeholder identification and strategies for security leaders. | Here, I supported group members and add strong advice on the industry analysis for the implementation of GenAI. The implementation of GenAI for the security purpose is essential these so I studied different industry where GenAI can be implemented and decided to choose automobile industry. I identified the external and internal stakeholders in automobile services and recommended the security guidelines for the safe and secure use of GenAI in automobile services. | Provided the brief description of automobile service industry, categories the stakeholders inside the industry and set od security strategies are there for the implementation of GenAI. |
| Flowchart/System design/Network-Security architecture | These are the pictures that I have designed based on the project scenario and requirements that I have attached to the project report. | These pictures provide the understanding of project through the diagram. |
| AI tool development. | I have a significant contribution for the development of AI including coding for the AI program, using ML AI model, vulnerability testing areas. | I have generated a program for AI model for cybersecurity vulnerability scan. |
| Website hosting. | I have hosted a website designed by other group members into the AWS web server. |  |

# Newly Developed Skills

There were several challenges and opportunities for the completion of the project. This project really helped to gain new knowledge and the way to tackle the challenges and handling pressure. Here, I have short-listed the newly developed skills while completing the project.

|  |  |  |
| --- | --- | --- |
| **Skills** | **Related tasks** | **Justification** |
| Critical thinking and analytical skills. | * Preparing report. * Increase reading and writing ability. * Increase problem solving ability. * Think out of the box. * Gaining new knowledge. | I realised that my critical thinking and analytical skills have been increased once when I started working on this project. This is because I have gone a lot of content and tried to understand line by line while preparing report for the project. |
| Research and reading skills. | * Preparing report. * Increase reading and writing ability. * Increase problem solving ability. * Think out of the box. * Gaining new knowledge. | I have read few articles related to use of Gen AI in terms of cybersecurity vulnerability, I would say that the boosted the capacity of mine reading ability and understand of their meaning and correlate to the project topic. |
| Programming skills. | AI development and other application. | I had a basic understanding of programming language python before, this project forced me to work upon it with giving my best. I have watched couple of videos on YouTube to overcome the issues arises during program coding. |
| Web hosting. | Website hosted on AWS. | This task was new for me, I would say this is the best task I have done during the project. I have gone through couple of videos on YouTube to get an idea. Thankfully, I am able to deploy website on AWS web server using EC2. |
| Skills on cybersecurity analysis | Analyse and evaluate the cybersecurity vulnerability scan report. | The project has demonstrated the AI tool using machine learning model to detect the cybersecurity vulnerabilities that generate the scan report. The report shows the possibilities of occurrence of different vulnerabilities such as sql injection, brute force attack and anomalies detection. |

# Application of Existing Skills

The above-mentioned skills have broader application over the information and technologies and applicable for tackling the day-to-day challenges. Here, I have listed the areas of applications of above-mentioned skills.

|  |  |  |
| --- | --- | --- |
| **Skills** | **Related tasks** | **Justification** |
| Critical thinking and analytical skills. | * Preparing report. * Increase reading and writing ability. * Increase problem solving ability. * Think out of the box. * Gaining new knowledge. | This skill may be applicable on preparing a report writing and collect the information regarding the project topic. Critical thinking and analytical skills increased the thinking out of the box and find the solution of the problem as fast as possible. Analytical skill helps to find the core meaning of the topic and go deeply to analysis the topic related findings. |
| Research and reading ability. | * Preparing report. * Increase reading and writing ability. * Increase problem solving ability. * Think out of the box. * Gaining new knowledge. | Research and reading ability may increase the knowledge areas and helps in thinking broader. It is also applicable in time management and correct utilization of time and finding the correct information related to the topic. |
| Programming skills. | AI development and software application development. | Basically, the knowledge of programming language is applicable on the design and development of website and software development. |
| Website hosting. | Host website in AWS or any other web server. | This skill is applicable on hosting website on any web server specially if you are website developer or software developer. |
| Skills on cybersecurity analysis. | Analyse and evaluate the cybersecurity vulnerability scan report. | The incidents of cybersecurity attacks are the major concerns now a days. So, the skills of analysing and evaluating cybersecurity vulnerability has bright future. |

# Contribution of Team Members

I would say that all team members in a group contributed equally. If I have rank them randomly, here is the list of group members who contributed from best contribution to least contribution.

1. Bhuwan Thapa
2. Basanta Adhikari
3. Pratik Singh Dhami
4. Kiran Bhusal

I would like to express that Bhuwan Thapa has the best contribution through out the group project completion. Because of the reason that, he has contributed on significant areas of the project such as best contribution to prepare the project report to keep tracking the project progress, developing technical artefacts to drawing the diagram for the project report and arranging the team meeting to analysing the meeting outcomes. Apart from that Basant Adhikari has also contributed equally to the project progress such as report writing to managing project plan and also contributed on technical progress of the project. At last, others team members also have significant contribution for the project, they equally contributed on report wring and technical development of the project.

# Reflection on Project Experience

The fascinating part of the project was analysing the dual nature of the GenAI such as short-term skepticism and long-term promises in the cybersecurity domain. Analysing how GenAI such as ChatGPT and Gemini can support to enhance cybersecurity measures with preventing risks was also excited. Another interesting part of the project was developing and learning the new skills such as website design and development and development of AI tool for vulnerability detection. The implementation part was difficult but once when it gets success the excitement and satisfaction was in different level.

Previous knowledge from networking and cybersecurity courses proved invaluable. Understanding core cybersecurity concepts and network architectures provided the solid foundation for the technical implications of integrating GenAI into cybersecurity system. This background knowledge helped in developing the comprehensive framework for ethical AI implementation and risk assessment strategies.

There were multiple significant hurdles encountered while completing the project, the one was balancing the technical aspects of GenAI into broader business and ethical considerations. Addressing issues like intellectual property concerns, economic disruptions and managing shareholders expectations and other technical required extensive research. There were difficulties on the development of AI tool such which method is used for the vulnerability detection, which machine learning AI model can be used etc. Another hardest part of the project was developing the risk assessment and mitigation plan. Creating thorough threat, vulnerability and asset (TVA) analysis for GenAI implementation in cybersecurity required deep consideration of risk and their impacts.

I expect, this experience will be helpful in future cybersecurity roles. This project has provided the comprehensive understanding of how emerging technologies like GenAI can be integrated into security practices for managing associated risks. The skills developed in ethical framework creation, risk assessment and stakeholder communication will directly be applicable in real world scenarios.

If given the opportunity to do this project again, one area for improvement would be to incorporate more real-world case studies of GenAI implementation in cybersecurity. While this project is based on theoretical part more, it would better to provide practical examples that includes challenges and successes experienced by organization who have already utilized these technologies. Additionally, expanding the collaborative training programs to include more interactive elements, hands-on workshop with GenAI tool could enhance its effectiveness. This world provides more immersive learning experience for both technical and non-technical staffs.

In conclusion, this project has been a valuable learning experience, combining theoretical knowledge with practical applications in the field of GenAI into cybersecurity. It has provided the holistic approach to technology implementation, considering not only technical aspects but also ethical, business and human factors. The skills and insights gained from this project will undoubtedly prove beneficial in navigating the complex and evolving future of cybersecurity in the time of artificial intelligence.

# Portfolio Contribution

The project topic name “GenAI: Navigating Short-term Skepticism and long-term Promises” address about the current challenges and opportunities presented by GenAI in cybersecurity. This project particularly talks about the challenges and opportunities in the cybersecurity of automobile services, where this project presents the sets of security guidelines for security leaders, provide ethical AI frameworks, risk assessments and mitigation plans and training needs analysis for technical and non-technical staffs in the automobile services industry mainly focusing on the implementation of GenAI into cybersecurity. For my contribution to technical development of the project, I lead the for the development of AI tool which detects cybersecurity vulnerabilities and designing and hosting the website on web server.

Here I have provided the link of my e-portfolio, where I have listed the project task, project development, technical development and my contribution over the completion of project and other achievements.

e-portfolio link - <https://portfolium.com/BhuwanTHAPA>

GitHub link - <https://github.com/kiransun/Generative-AI.git>