

Project Proposal

by Josh Lloyd

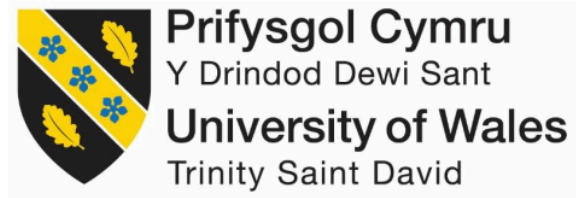
Submission date: 21-Oct-2024 02:35PM (UTC+0100)

Submission ID: 240767864

File name: 40810_Josh_Lloyd_Project_Proposal_586419_1174047978.docx (123.16K)

Word count: 1983

Character count: 10418



A Study of the use of AI in the assistance of security within networks

by

Joshua Lloyd

Supervisor: Nitheesh Kaliyamurthy

Project submitted as part of the requirements for the award of

BSc (Hons) Computing (stream)

BSc (Hons) Networks & Cybersecurity

April 2025

DECLARATION

I, Joshua Lloyd declare that I am the sole author of this Project; that all references cited have been consulted; that I have conducted all work of which this is a record, and that the finished work lies within the prescribed word limits.

This work has not previously been accepted as part of any other degree submission.

Date: 28/09/2024

FORM OF CONSENT

I Joshua Lloyd hereby consent that my Project, submitted in candidature for the B.Sc.(Hons) Computing (stream) degree, if successful, may be made available for inter-library loan or photocopying (subject to the law of copyright), and that the title and abstract may be made available to outside organisations.

Date: 28/09/2024

Table of Contents

DECLARATION	2
FORM OF CONSENT	2
1. Introduction.....	4
2. Background to the Proposed Research.....	4
3. Research Problem statement.....	5
4. Research Aim & Objectives	5
5. Methodology.....	6
5.1 Methods.....	6
5.1.1 Research philosophy.....	6
5.1.2 Research methods	6
5.1.3 Research Strategy.....	6
5.1.4 Analysis and Evaluation Methods.....	7
5.2 Materials.....	7
5.2.1 Details of Research Data:	7
5.2.2 Sources	7
5.2.3 Hardware:.....	7
5.2.4 Software:	7
6 Project Plan	8
7. References	8

1. Introduction

This project aims to highlight the importance of integrating new and upcoming technologies into preexisting technologies and networks. Its focus is on using AI within networks to enhance security and how this can be achieved by using general-use AI to assist non-specialist individuals.

I would like to undertake this project because with all the new technologies being developed in recent years, people read about them and get scared by their potential. I would like to be able to alleviate some of this fear by trying to teach simple ways these technologies can be used to help keep individuals secure and also show them that it is not all bad.

I believe safety online is now more important than ever as there are new ways being constantly developed to breach systems so I would like to show people how simple it can be to take steps to keep themselves safe and I think there is a gap for this in research as it describes to people what the technologies are and what their potential is but it does not detail effective countermeasures and how technologies can also be used to great benefits even at an entry-level for non-specialist individuals.

At the end of this project, I would like to make a small handbook on how individuals can keep themselves secure online based on the research and experiments I will conduct throughout the duration of this personal project.

2. Background to the Proposed Research

Looking through previously conducted research AI is an upcoming technology in the networking sector although it is not yet fully implemented it does still have its uses however [1] found that most of them are too intricate and erratic for human cognition they also state that this lack of interpretation hinders the commercial success of AI-based solutions in practical practice they also state to work around this challenge AI researchers are exploring more explainable AI techniques what they have labeled as (XAI) these models are more interpretable, manageable and trustworthy. Although these AI have their uses these findings may prove challenging if believed to be true if the AI is not interpretable my participants will struggle with the experiment as they would not understand the AI.

Software-defined networking represents a huge networking architecture that combines management and programmability. [2] Finds that recently the research community has benefited greatly from advancements in the AI field to provide learning abilities and better decision-making and development in SDN.

This would be excellent for my experiment if this is to be believed this means that the AI may be able to learn how the network is structured and provide suggestions on how to enhance the security of the network.

Based on these two findings alone I believe there is a gap in research for my project although [1] talks about developing more interpretable AI it leaves out how that AI will be used and taught to its users or the general public which is what my project aims to achieve and based on [2,3] finding it could potentially be a very powerful tool to use when using it in a networking environment.

[5,6] Finds that AI programs generally work by analyzing massive amounts of data generated by network traffic, and host processes and users to detect suspicious activities using algorithms however due to the huge data processing causes slow training and testing processes which can result in low detection rates. These findings prove although AI is a useful tool it is yet far from perfect and still requires human interaction however as it can still assist in these processes it is still a valid tool to use in a networking environment which I why even a general-purpose AI can be used to enhance security even if it's to a small degree I aim to test these capabilities and apply them to the network environment and use them to assist in the security enhancement to educate users on the potential they have and that is where I think my research will fit perfectly in the gaps.

3. Research Problem statement

My project aims to tackle the fear of developing technologies by using AI to enhance the security of a small network. This should be achievable by individuals who have no experience in a security field as this project is intended for general public use. The project should mirror a small home network to simulate the intended environment.

4. Research Aim & Objectives

The aim of the project is to educate untrained individuals on how to enhance the security of a small network by using AI software to educate/assist in the effort to correct security faults within the network.

- Develop/simulate a pre-existing network to conduct penetration testing within said network.

- Research capabilities of both general and specialist use AI applications
- Apply an AI to assist with fixing issues that arise during the penetration testing phase
- Record my findings and how the AI-assisted the patches
- Create a simple step-by-step instruction handbook on how general use AI can help assist in enhancing the security of small-scale networks (E.g. Home networks)

5. Methodology

5.1 Methods

5.1.1 Research philosophy

For this project I will be undertaking the interpretivism research philosophy as I believe it fits most with my project as I am testing human-software interaction which fits the model perfectly I believe that following this philosophy will serve me the best throughout the course of my project.

5.1.2 Research methods

For this project I will be using qualitative sources for my data collection I believe this fits most in line with the topic of my project as I will be using specialist equipment there are reliable sources that provide guides and manuals on how to operate and manipulate said machinery whether that be the manufacturer of the equipment itself or professionals in the fields of the equipment I believe by using information from these sources will provide me with the most useful and accurate information I will be able to find. And due to the project not using a how lot of numerical data a qualitative approach seems more fitting for the project.

5.1.3 Research Strategy

My research strategy for this project is going to be experimental as I am testing the relationship between humans and the use of artificial intelligence.

Hypothesis:

Can general use AI be used to enhance the security of networks?

My independent variable is going to be the network system when the alterations are made from AI assistance and my dependent variable is going to be the participants of the experiment I want to measure if the AI can educate the participant to make alterations to the security of the network to test for any weaknesses.

5.1.4 Analysis and Evaluation Methods

Upon conducting my experiments and gathering my data I will analyze and cross-examine my research with research I found in my literature review and others and highlight the gaps that my research would fill and how it can help individuals at an entry-level I will also ask my participants to fill in feedback forms to see if what they learned helped and what they would improve about the process or experiment this will help me refine my project for a final review and highlight any problem areas that happened during the experiment.

5.2 Materials

5.2.1 Details of Research Data:

I will be gathering my research data from journals and articles in the area of AI software and their applications I will use this research to further my own understanding before conducting the experiment I will be under obligation to reference and cite these sources as I would need to credit the material as it is not research I would just be basing my research off of said sources.

5.2.2 Sources

-UWTSD library

-Google Scholar

I will be using these two as my sources as they both provide a vast library of research journals and articles related to my topic of study and will be the best place to find said sources.

5.2.3 Hardware:

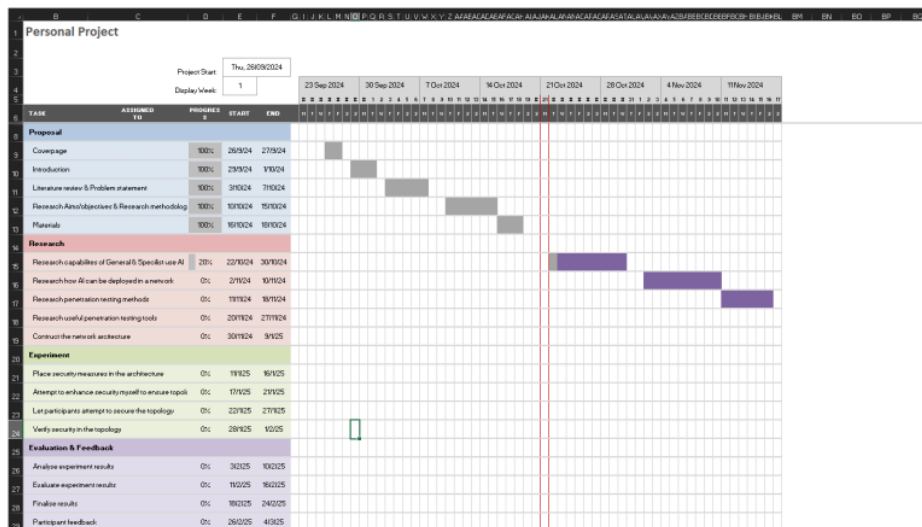
- Desktop PC's
- Cisco routers
- Cisco switches

5.2.4 Software:

- Cisco packet tracer
- Wireshark
- ChatGPT

- Open AI

6 Project Plan



7. References

References

- [1] T. Zhang, H. Qiu, M. Mellia, Y. Li, H. Li and K. Xu. T. Zhang, H. Qiu, M. Mellia, Y. Li, H. Li, and K. Xu. Interpreting AI for networking: Where we are and where we are going. *Interpreting AI for networking: Where we are and where we are going. IEEE Communications Magazine IEEE Communications Magazine* 6060(2), pp. 25–31. pp. 25–31. 2022.

Available: <https://ieeexplore.ieee.org/abstract/document/9722797>. DOI: 10.1109/MCOM.001.2100736.

[2] L. Song, X. Hu, G. Zhang, P. Spachos, K. N. Plataniotis and H. Wu. L. Song, X. Hu, G. Zhang, P. Spachos, K. N. Plataniotis and H. Wu. Networking systems of AI: On the convergence of computing and communications. Networking systems of AI: On the convergence of computing and communications. *IEEE Internet of Things Journal* *IEEE Internet of Things Journal* 99(20), pp. 20352–20381. pp. 20352–20381. 2022.

Available: <https://ieeexplore.ieee.org/abstract/document/9766416>. DOI: 10.1109/JIOT.2022.3172270.

[3] M. Latah and L. Toker. M. Latah and L. Toker. Artificial intelligence enabled software-defined networking: A comprehensive overview. Artificial intelligence enabled software-defined networking: A comprehensive overview. *IET Networks* *IET Networks* 88(2), pp. 79–99. pp. 79–99. 2019. .

[4] S. A. Latif, F. B. X. Wen, C. Iwendi, L. F. Wang, S. M. Mohsin, Z. Han and S. S. Band. S. A. Latif, F. B. X. Wen, C. Iwendi, L. F. Wang, S. M. Mohsin, Z. Han and S. S. Band. AI-empowered, blockchain and SDN integrated security architecture for IoT network of cyber physical systems. AI-empowered, blockchain and SDN integrated security architecture for IoT network of cyber physical systems. *Computer Communications* *Computer Communications* 181181pp. 274–283. pp. 274–283. 2022.

Available: <https://www.sciencedirect.com/science/article/pii/S0140366421003662>. DOI: 10.1016/j.comcom.2021.09.029.

[5] M. Waqas, S. Tu, Z. Halim, S. U. Rehman, G. Abbas and Z. H. Abbas. M. Waqas, S. Tu, Z. Halim, S. U. Rehman, G. Abbas and Z. H. Abbas. The role of artificial intelligence and machine learning in wireless networks security: Principle, practice and challenges. The role of artificial intelligence and machine learning in wireless networks security: Principle, practice and challenges. *Artif Intell Rev* *Artif Intell Rev* 5555(7), pp. 5215–5261. pp. 5215–5261. 2022.

Available: <https://doi.org/10.1007/s10462-022-10143-2>. DOI: 10.1007/s10462-022-10143-2.

[6] R. Patel, H. Mistry, A. Goswami and C. Mavani. R. Patel, H. Mistry, A. Goswami and C. Mavani. Artificial intelligence for networking. Artificial intelligence for networking. *Educational Administration Theory and Practice* *Journal Educational Administration Theory and Practice* 3030pp. 813–821. pp. 813–821. 2024.

Available: https://www.researchgate.net/profile/Ripalkumar-Patel/publication/383061131_ARTIFICIAL_INTELLIGENCE_FOR_NETWORKI

[NG/links/66c137888d007355925dbdf8/ARTIFICIAL-INTELLIGENCE-FOR-NETWORKING.pdf.](#)

Project Proposal

GRADEMARK REPORT

FINAL GRADE

GENERAL COMMENTS

75/100

PROJECT PROPOSAL – ACCA6020 INDEPENDENT PROJECT

Student Josh

Lloyd

Mark...75

Intro / A&O (400 words)		
Project title; Identification of a specific problem to be investigated; Well-defined aims and SMART objectives; Explaining why this project is worth doing; Discussion of what the project needs to do in order to be a success; Description any deliverables that will be produced at the end of the project	20	16
It's a good idea you're proposing; however, the scope is currently quite broad, and you might not be able to accomplish all your goals within the given timeframe. Conducting penetration tests and offering mitigation is a project on its own, so		

moving on to creating a handbook might add extra work. Why not take some of the content you wanted to cover in the handbook and find a way to summarize it, fitting it into the project's Recommendations and Conclusion sections instead		
Background to the Project / Literature Review (400 words)		
Description of how the work to be done by in the project relates to the work identified in the literature review; Discussion of any ethical issues raised by the project Identifying what has already been done within the field; Topic familiarity; Brief literature review using appropriate sources – 6-8 journal papers and book chapters rather than just websites; Selection of relevant models & concepts		
You provided a clear background to the project, but I was expecting you to reference about 6-8 journal papers; you used about 5, which isn't that bad. However, you were a bit general about how current AI is being used to enhance security in SDN. You really need to conduct more research on the related work for your project. Additionally, this section was also supposed to address any ethical issues.	20	14

Project Design (500 words)		
Clear statement of which development methods are to be used and why they are appropriate; Clear statement of which tools are to be used and why they are appropriate; Clear description of how data collected will be analysed It's good that you discussed the research philosophy and research methods. However, you could have included a diagram providing an overview of exactly what you will be doing in your experiments. You listed the tools, but did not explain why they are appropriate.	30	21
Resources / Planning (200 words)		
List of any deliverables; Clear diagram showing both timing and resource use; Completed ethics form; Limited and relevant appendices although you mentioned the necessary hardware and software resources, you were also expected to list any deliverables. It's good that you included a Gantt chart to show timing and resource use, and you should be	15	12

commended for completing the ethics form as well.		
Document Presentation		
Correct spelling, grammar and punctuation; Flow of narrative/fluency; Coherence; Word processed ; Correct use of referencing with bibliography; Strict word limit The document was professionally created, with many sections adhering to the word limit. It's great that you included a table of contents page.	15	12
TOTAL	100	75

PAGE 1
PAGE 2
PAGE 3
PAGE 4
PAGE 5
PAGE 6
PAGE 7
PAGE 8
PAGE 9
PAGE 10