**Determining if cyberattacks can be detected and analysed by using network logs from devices**



Myron Furtado

19703402

19703402@students.lincoln.ac.uk

I want to know if DDoS attacks be detected using network log data

School of Computer Science

College of Science

University of Lincoln

Submitted in partial fulfilment of the requirements for the

Degree of BSc(Hons) Computer Science

*Supervisor:* Dr Yvonne James

April 2022

**Acknowledgements**

Firstly, I would like to thank my supervisor Yvonne James that has been there to help me with ideas when looking for the topic and then answering questions. I would also like to thank my Tutor, Dr Heriberto Cuayahuiti for doing team meeting with me and being supportive when I was thinking about how to approach this project.

**Abstract**

Cybersecurity attacks and network anomalies can cause massive damage to individuals/organisations/companies affected based on the scale of the attack. The attacks can result in both financial and reputational damage

Write this at the end

Keywords: Cyberattacks, network logs, Log file analysis, Network anomalies, NetFlow data, Machine learning Models, Classifying data, Cybercrime

**Table of Contents**

[Introduction 1](#_Toc104290865)

[1.1 Introduction to the Cyberattacks 1](#_Toc104290866)

[1.2 Main ideas to be examined, developed and discussed 3](#_Toc104290867)

[1.2 Aims 4](#_Toc104290868)

[1.3 Objectives and Milestones 4](#_Toc104290869)

[Literature Review 5](#_Toc104290870)

[2.1 Background 5](#_Toc104290871)

[2.2 DDoS attacks 5](#_Toc104290872)

[2.3 New emerging technologies to combat cyberthreats 7](#_Toc104290873)

[Methodology 10](#_Toc104290874)

[3.1 Project Management 12](#_Toc104290875)

[3.1.2 Gantt chart 14](#_Toc104290876)

[3.1.3 Risk Assessment 16](#_Toc104290877)

[3.1.4 Supervisor Meetings 16](#_Toc104290878)

[3.1.5 Evaluation Methodologies 16](#_Toc104290879)

[3.2 Software Development 18](#_Toc104290880)

[3.3 Toolsets and Machine Environments 18](#_Toc104290881)

[3.4 Research Methods 18](#_Toc104290882)

[Design, Development and Evaluation 19](#_Toc104290883)

[4.1 Software Development Projects 19](#_Toc104290884)

[4.2 Research Projects 20](#_Toc104290885)

[Conclusions 21](#_Toc104290886)

[Reflective Analysis 22](#_Toc104290887)

[References 23](#_Toc104290888)

[Word Count 25](#_Toc104290889)

**List of Figure**

[Figure 1- Common motivation behind Cyberattacks bar chart (Alghamdie, 2021, 4) 2](#_Toc104222745)

[Figure 2- Basic SDN Architecture (Sahoo et al., 2019) 7](#_Toc104222746)

[Figure 3 -Waterfall PM model stages (Cohen, 2022) 11](#_Toc104222747)

[Figure 4 -Agilel PM model stages (Cohen, 2022) 12](#_Toc104222748)

[Figure 5- Five phases of Project Management (Friedman, 2020) 12](#_Toc104222749)

**List of Tables**

[Table 1: The table below considers the risk involved in different Project management models Risk assessment 17](#_Toc104294738)

[Table 2 - Project management (PM) model comparison. 19](#_Toc104294739)

**Chapter 1**

# Introduction

## Introduction to the Cyberattacks

The internet is a vast space that has changed our world. It has reshaped technology, businesses, human interactions, society, and information exchange. Around 10 billion devices are connected to the internet as of recently. This however also increases the number of devices that can be at risk of being attacked and compromised. Cyberattacks can come in many forms such as Viruses, spyware, phishing attacks and so on. The attackers are after sensitive information so they can share it publicly or hold it at Ransome for financial or personal gain (Alghamdie, 2021). For companies, cyberattacks can add significantly to their operating cost by requiring additional security measures, litigation costs, fines and penalties, not to mention the loss of customers and reputation (Kamiya et al., 2021, 721). The figure below breaks from a 2012 study that breaks down the common motivation of attackers based on what they want. And the most prevalent reason, at 30% is to gain access to private/personal sensitive information.

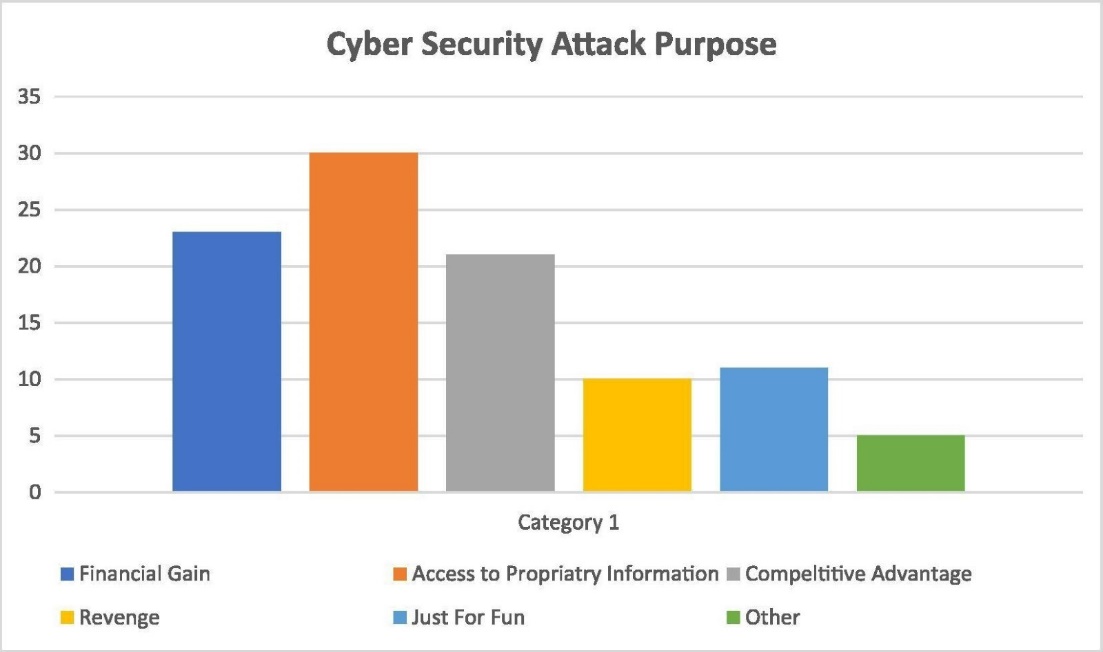


Figure 1- Common motivation behind Cyberattacks bar chart (Alghamdie, 2021, 4)

There are many types of attack vectors such as DDoS attacks, Viruses, spyware, SQL injections and so on. The attackers are after sensitive information that can either be made public or held at ransom till, they get paid to return the information (Alghamdie, 2021). For companies, cyberattacks can add significantly to their operating cost by requiring additional security measures, litigation costs, fines and penalties, not to mention the loss of customers and reputation (Kamiya et al., 2021, 721).

One method of detecting cyberattacks is to perform real-time analysis of network traffic and system files, but this is a very difficult process and cannot be relied upon a 100%. System Log analysis is another way of checking what has happened in the system as they provide concrete proof of the activities that happened in the machine. One of the newest methods of detection is the training of machine learning/deep learning models to learn and detect cyberattacks (Liu et al., 2021, 10985). To ensure that the models were making credible detections they are compared to the results of other methods of analysis (Liu et al., 2021, 10985). Deep learning and machine learning methods are far from perfect but are improving every day.

This project will try to study/analyse network log data using datasets collected by me from a Mac or Windows machine. It will contain network packet data received/sent from the machine, collected when a cyberattack was happening. This is supposed to identify abnormalities/irregularities in the network traffic data. I am confident this project will give me insights into some areas of the job role of a network engineer. As I am interested in applying for this role after completing university.

## Main ideas to be examined, developed and discussed

The main question asked in this project is if cyberattacks can be detected by performing an analysis of network data that is recorded from the concerned computer. Cyber attacks come in many forms but this project will focus only on Denial of service (DoS) and Distributed Denial of Service (DDoS) attacks as going diving into other threats will greatly increase the size of the project. This is because not every threat can be detected using the same model, each threat needs a threat specific technology to be detected. DDoS attacks are very common on corporate entities and government agencies.

The DDoS script used for this project is not very powerful but still does send quite a lot of HTTP flood traffic over to the target. This script will perform the DDoS attack on the target device. Wireshark is a packet sniffer tool available on Windows and macOS, both of which have been used in some stages of the project as the target devices. Using Wireshark network data was collected. Wireshark allows the user to record many components of network traffic data. For example, the project dataset needed the source and destination port numbers in the exported file, so these had to be selected during the export process. The data is then run through a Machine learning model. In the project, the Machine learning model that was used is called k-nearest neighbour/KNeighborsClasifier as it can predict the dataset used with really good accuracy. Enter here what model is used and explain further

Research questions that need to be addressed?

## 1.2 Aims

This project aims to analyse and study Network packet log data by utilising Machine learning models to do the analysing and make the decision. This will help to determine if the machine models selected can be used to detect traces of DDoS attacks from the network packet logs. The data is collected on a macOS device as the target and the DDoS attack was performed on a Windows system using a python script.

## 1.3 Objectives and Milestones

1. Conduct a thorough Literature review
2. Research how to code a DDoS script, then code it in python
3. Test the DDoS script to make sure it works
4. Research what program to use to collect the Network log data
5. Launch DDoS attacks and record the resulting log data
6. Clean the Recorded data to remove Null, None and empty values
7. Select a Machine learning model from Scikit-learn to use for analysing data
8. Code the Machine learning part of the project, which includes importing the dataset to X and Y matrices, splitting the new dataset matrix into test and train, and training the model
9. The Model should output data that need to be displayed to the user. E.g., If DDoS has been detected or not, graphs breaking down and visualising the input dataset- IP address breakdown, port breakdown and so on
10. Write up the Final report explaining the process

**Chapter 2**

# Literature Review

## 2.1 Background

Network logs can be analysed using machine learning algorithms to detect abnormalities in the log data. These models can then be used to predict cyberattacks. Bad actors can gain access to network systems through the network with the intent to cause disruption, breakdown, operational failure, and service interruptions. Studies such as (Ning and Jiang, 2021, 1154) have studied well-documented cyberattacks including Stuxnet on Siemens and Black energy that affected electrical grids in Ukraine. Both incidents caused physical and financial damage. One way to tackle this would be to use application network monitoring software but attacks on the hardware level will slip by undetected in this case, a better way to boost network security would be to study the network logs and analyse the data.

## 2.2 DDoS attacks

The internet has revolutionized the world since its inception. In their paper (Musumeci et al., 2021) say “it reshaped the technology, business communication, society, economic and many more.” They also note that it increases the level of risk for users connected to the internet. Distributed denial of service (DDoS) attacks are very dangerous for servers and systems that are connected to the internet. They explain that in a DDOS attack the attacker sends massive amounts of malicious traffic to cause the CPU or NIC (Network interface card). (Musumeci et al., 2021) notes that multiple vectors of attack can be deployed using dynamic/spoofed IP addresses to perform a combined attack and since there are massive numbers of IP addresses coming in making it is difficult to block them all by backlisting IP addresses consistently. “The most utilized DDoS attacks are typically grouped in the following categories: TCP SYN flood, UDP flood, ICMP flood and HTTP flood”. Another serious type of DDoS attack is the TCP SYN attack which is used a lot in today’s environment. This attack exploits the “TCP connections’ initiation packets to target the victim” (Musumeci et al., 2021). They discovered three ways to prevent and mitigate DDOS attacks. These are:

* Source based detection, where the incoming IP addresses are blacklisted
* Destination based detection, where the target system performs detection
* Network-based detection, where switches and routers are used to detect incoming attacks

In their paper (Musumeci et al., 2021) perform network-based detection by implementing defence mechanisms at the SDN (Software defined network) switches and block traffic at the data plane level while also saving the SDN controller from breakdown or going out of service.

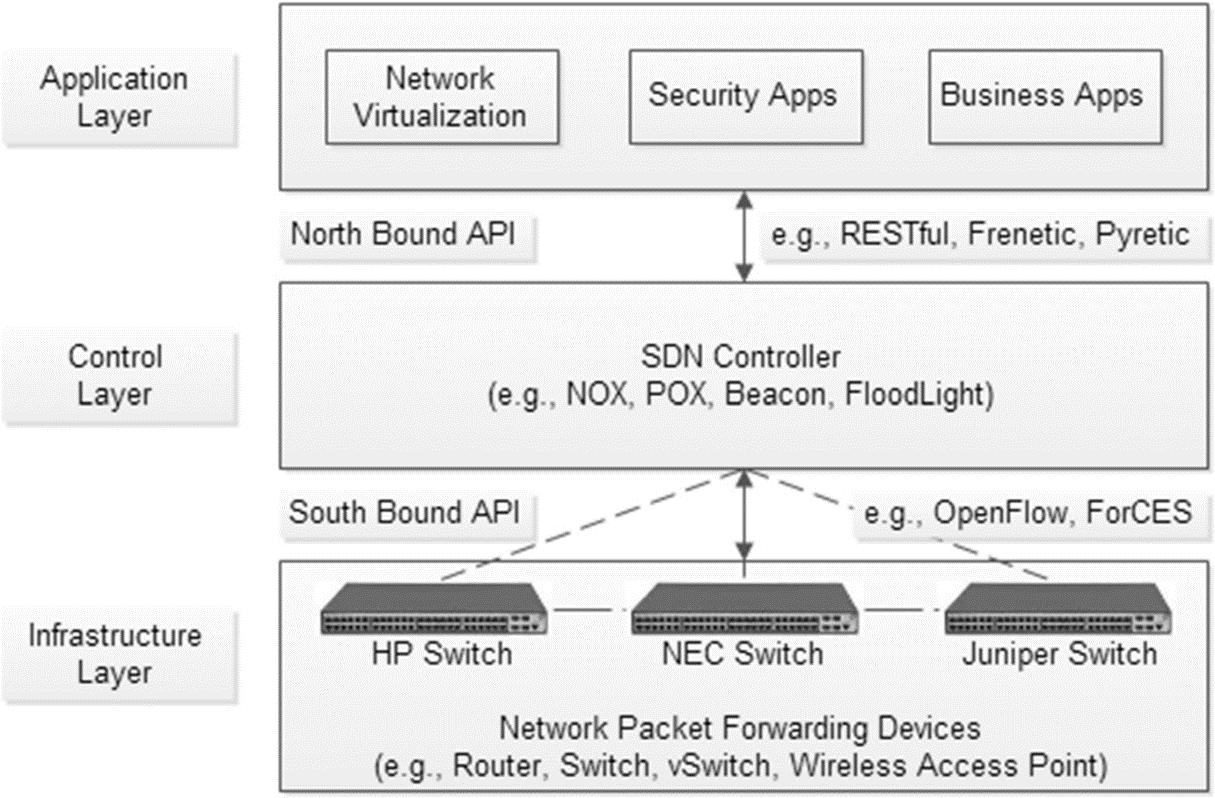


Figure 2- Basic SDN Architecture (Sahoo et al., 2019)

## 2.3 New emerging technologies to combat cyberthreats

Recent Developments: In their paper (Sahoo et al., 2019) they identified SDN (Software Defined Networks) as the new technology that many organisations need as a defence mechanism against cyber threats such as DDoS attacks. It helps solve network classification problems by using software to keep tabs on the traffic flow and root out DDoS or suspicious traffic. In my opinion, while this improves security it is not unbreakable as it is still possible to find new exploits in different layers of SDN. So, it is important to keep an eye on the logs in conjunction with SDN deployment.

The ELK stack is a package of open-source software (i.e., Elasticsearch, Logstash, and Kibana) that allows for the extraction of information for the log files and collects the required data metrics for processing (Liu et al., 2021, 10986). These provide a very concrete way of protecting potential high-risk targets like healthcare institutions. For example, healthcare devices can be vulnerable to Denial of Service (DoS) attacks due to the Software-defined Network (SDN) controller’s limitation with flow tables (Huertas et al., 2021, 2719-2720). These can be mitigated by using policy-based architecture for Multi-Access edge computing (MEC) that allows it to detect and protect against cyberattacks that exploit SDN’s weakness. This can help protect wearable health devices that are used by patients which will help save their lives and associated costs (Huertas et al., 2021, 2720). Research journals such as (Yang et al., 2019, 6344) have used log monitoring using the ELK stack to make networks safer. Collecting data for network logs and NetFlow logs using the Filebeats tool to convert the data to a visual format. Then combining that data with the NetFlow log data using the ceph file system (aka, CephFS) allowed them to compare the performance of the Reliable Autonomic Distributed Object Store (RADOS) gateway. This ensures that the people making the decisions on issues of network security have the most accurate, up-to-date, and safe information on the state of network security allowing them to make informed decisions.

Deep neural networks (DNNs) are Artificial intelligence models that are well known to be used for making predictions. First, DNNs are fed data (in our case network log data) and then the training data can be used on other test datasets to make predictions on the data we need to classify. DNN models do have a problem, when upper and lower neurons are fully connected the model can form a connection resulting in overfitting of the data (Vinayakumar et al., 2019).

The most cutting-edge technology being experimented on for providing a scalable cyberattack detector uses a deep neural network (DNN) as produced in the study by (R et al., 2019, 41525) the models used are flexible and effective at learning different types of unpredictable cyberattacks. The way the attacks are evolving requires a scalable fast-paced method of learning which facilitates the improvement of the algorithm which can accurately detect most of the attack types it has studied up to that point. The main advantage of using DNN is the vast number of datasets available out there that can be used to train the algorithm.

The project will need a plan to test if the analysis work can identify threats. This can be done by generating various attack scenarios to test if the systems fail to detect attempts of cyberattack. Second, it would be to test again with the highest intensity attack and lowest intensity attack to see what changes that could have (Ning and Jiang, 2021, 1156). The test results from here will be able to help give insight into what policies can be adopted to minimize and mitigate future attacks.

Another tool available for data visualization functionality that allows for tracking network traffic with more options for editing. This can then be aplite to machine learning models such as DNN. This advanced feature allows for real-time data management to interpret if a cyber-attack is taking place, if a cyberattack is happening then network administrators can be alerted to it. One downside of this is that the model can raise false positives.

Kozik developed a combo of NetFlow’s that contained a machine learning classifier, in which the Map reduce model is used. Before that Kiran and Chhabra investigated real-time classification of network data using a supervised model and achieved over 90% accuracy in correctly classifying their elephant and mice data. This model might be able to translate the accuracy of our dataset as well.

Add more images if possible

It Has to contain a critical review of some of the journals used?

**Chapter 3**

# Methodology

3K words

Project Methodology can be defined as a set of conventions that a team working on a project agrees to follow while working on a project. In their book, they explain that project management is meant to make better use of the existing resources by making the workflow horizontal as well as vertical (Kerzner, 2003). They explain Project management is the planning, organising, directing and controlling of resources to split up the objectives and complete them as set goals/objectives. This requires the project manager, in this case, just me since it is an individual project assigning a completion date for each objective. Since this is an individual project the project management does not allow for vertical scaling (e.g., assigning more people to a team). The project can only be completed faster by utilising horizontal scaling (e.g., working on more than one objective/task at a time). This can cause difficulties during project progression since there aren’t other team members to check my progress and keep me in line making sure I am hitting my deadlines for the individual tasks. This could contribute to me losing sight of key goals and deviating from my original aims and going beyond the scope of my original project framework. This makes the Project management lifecycle (APM) necessary to increase the chance of successfully completing the project and set proper time management for it.

There are many different types of methodologies present out there that can be used for this project, each with its advantages and drawbacks. Their blog (Cohen, 2022) lists the following methodologies:

1. The waterfall methodology was created in the 1970s. It needs the project team to know the requirements before progressing further. The model is split into individual stages and each of them is self-isolated and it does allow the project to move to the next stage without completing the previous stage. If the project runs into an error, then the whole project plan needs to start back from the start. On the other hand, the model makes it easy to understand and complete the project stage by stage

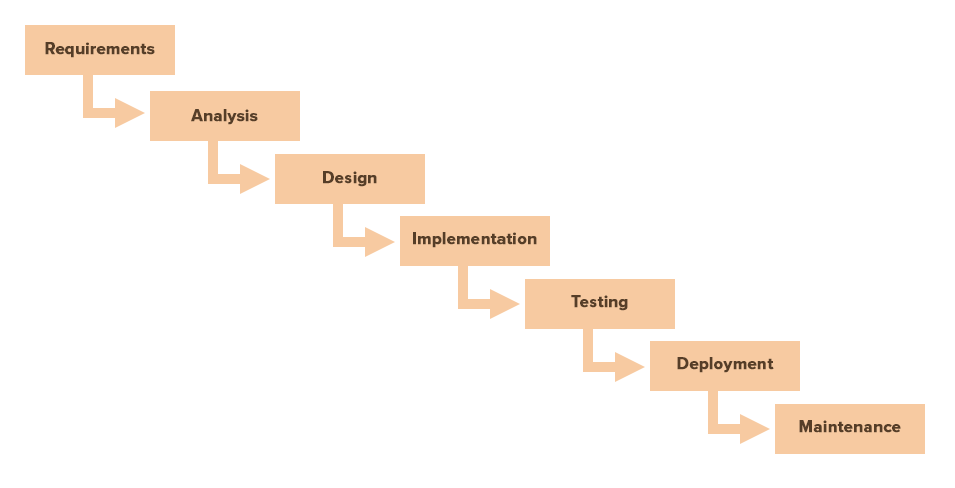


Figure 3 -Waterfall PM model stages (Cohen, 2022)

1. Agile is another “software development focused technology” (Cohen, 2022) for managing more complex projects. This method allows for more fast and flexible changes to the aims and objectives of the project as new issues are encountered. Unlike the Waterfall method complete requirement-gathering is not compulsory and the team can make small changes as the requirements change. On the other hand, this method does not have a fixed plan and can easily cause problems with scheduling and time management.

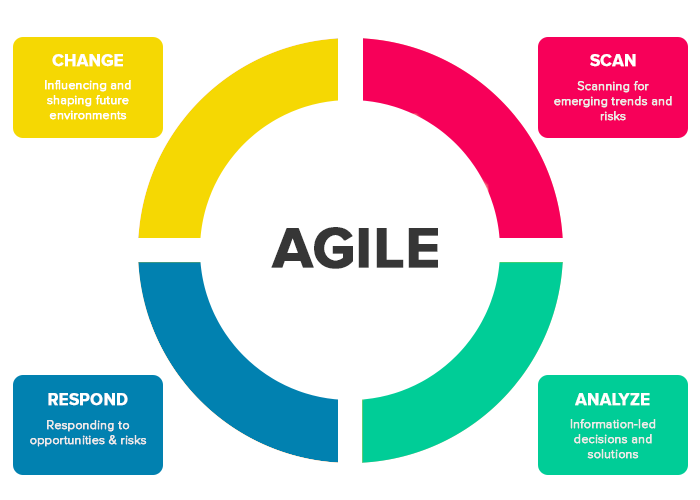


Figure 4 -Agile PM model stages (Cohen, 2022)

## 3.1 Project Management

This section will be used to discuss some of the tools and project management techniques that were available for use and discuss which ones were used or not used.

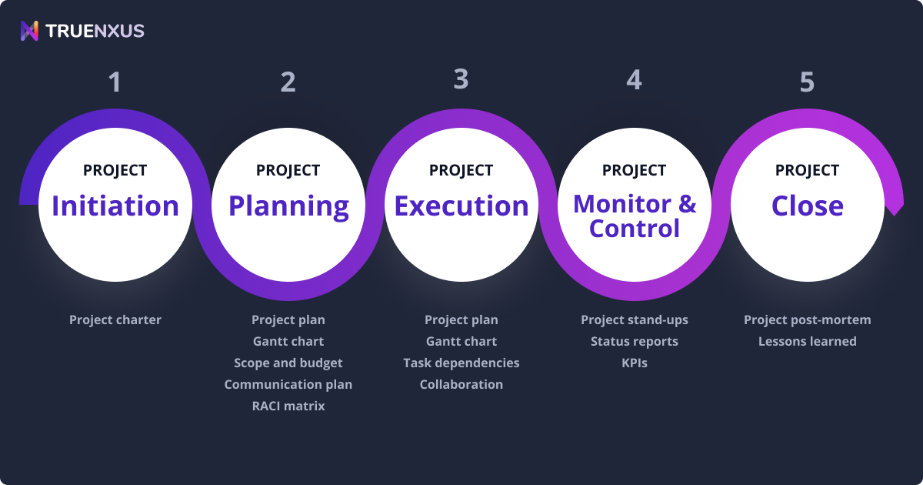


Figure 5- Five phases of Project Management (Friedman, 2020)

Based on the 5 phases of the PM model the following aims were drawn up to start the project, they are listed below:

* Conduct a literature review to find learn about the subject and technologies involved
* Requirement gathering and making a list of things to set up before starting coding
* Research and code the DDoS script that will be required to collect the DDoS dataset needed for the next step
* Run the DDoS attack and collect the dataset
* Clean the dataset and export it to the required format
* Import libraries needed to perform the setup for the Machine learning environment
* Make a requirement list of what the Machine learning model should output
* Code the Machine learning model. Includes data pre-processing, training model, using the trained data on the test set, and output of the desired results on the screen
* Test the Machine learning model under different conditions
* Wire the final report and fulfil other requirements

**3.1.1 Project management principles/Project Characteristics**

This project is fundamentally not normal as normally it would be a team of people working on different tasks and then bringing it together to finish it, but here it is an individual project, it is only going to be me that manages the project all through the process.

As the sole author of the project, they also do not have much experience in both areas of the project, they will have to learn how to perform DDoS attacks, collect log data and Perform Machine learning operations. Sufficient time should be allocated to work on the Machine learning section of the artefact. Since these are relatively new topics for the user there will be a learning curve before they become proficient at programming DDoS scripts and machine learning programming.

The project also has a deadline which limits the amount of time that is available to complete the project. The author does not however have to worry about the budget of this project as most of the requirements and tools needed are either open source or available freely. The budget is therefore going to be very low or free of cost altogether.

The project overall had its major objectives all listed in the proposal but the smaller objectives were not decided on at the start. As the result of previous tasks would decide what the next task to do would be. An example of this is cleaning the DDoS dataset would require collecting the DDOS dataset first, that in turn would rely on having a DDoS script. This meant the projects had realistic and quantifiable goals but the smaller tasks to do were not clearly defined at the start.

Project scheduling was handled using a Gantt chart that had most of the main tasks that need to be carried out to complete this project and each task and section has due dates. Some of the tasks were planned and worked on in parallel to reduce the time spent on implementing the project artefact.

## 3.1.2 Gantt chart

A Gantt chart was created at the start of the project and submitted along with the Project Proposal, it contained most of the tasks that needed to be performed to complete the project and each task had a start and end date assigned to it. The chart was also separated into 3 sections based on the work that needed to be done for the 3 individual assignments that this project is comprised of and each section also had its due dates. These task entries were then updated as each task was progressed through and completed. The updated Gantt chart is shown in the figure below.

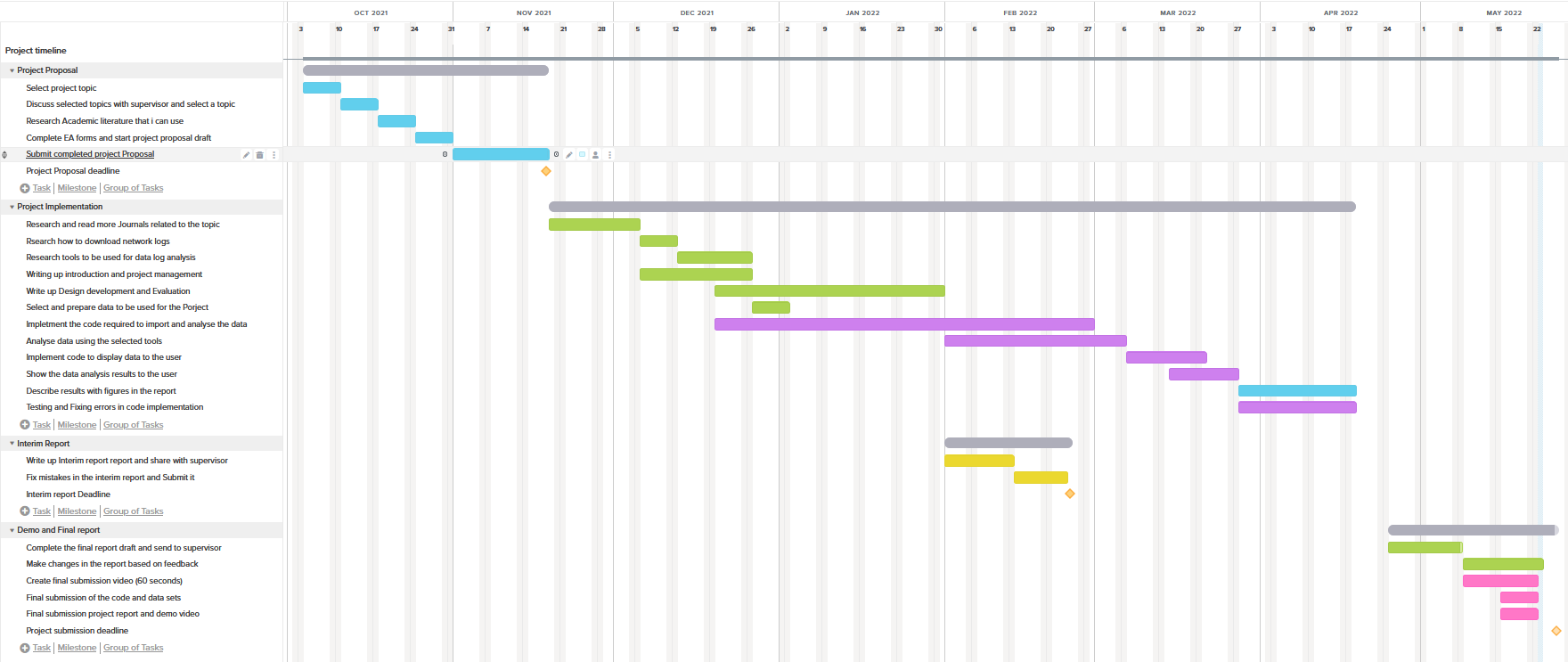


Figure 6- Project timeline Gantt chart after completion

The Gantt chart was created to show the time scale that the tasks were to be completed but it is not completely accurate and might be missing some of the smaller tasks undertaken to add toward the completion of the project. Some of the tasks were completed earlier than expected. For example, researching academic literature was completed a week before its due date, also writing up the Interim report was completed weeks before the deadline date. At the same time not, all task progression was properly marked and documented. For example, writing up the Introduction, Project management was supposed to be finished by end of December but was not fully completed even by the 25th of May. It was the same case with writing up the section about Design development and evaluation that was supposed to be partially completed by the end of January but was not fully completed by the 25th of May. And lastly, the task where the machine learning model had to be implemented is called “Implement the code required to import and analyse the data” so the name here does not properly explain what the task accomplishes. Also, it was supposed to be completed by the end of February but, actually was not fully completed before the 15th of May.

The advantage of utilising a Gantt chart for this project was that it displayed a detailed view of all the big tasks and most small tasks that needed to be accomplished making it very difficult to miss tasks and milestones that needed to be worked on and what each task flow looks like. Conversely, the bigger tasks encompassed smaller tasks that were combined to complete the big task this means that the big task needed further planning to show what tasks needed to be done at the lower level. For example, the biggest task “Implement the code required to import and analyse the data” which is the Machine Learning implementation included lower-level tasks such as:

1) Import the .CSV format DDoS dataset file

2) Perform data pre-processing

3) Print dataset information and useful plots that helps the user understand the dataset

4) Split the input dataset into test and train datasets required for the machine learning model

5) Implement the machine learning model

6) Train the machine learning model on the training dataset

7) Test the trained model on the test DDoS dataset

8) Display the predictions made

The smaller steps above are the breakdown of the one step shown in the Gantt chart. It was not feasible to mention all these small steps in the Gantt chart so it tends to show generic overviews in some sections.

## 3.1.3 Risk Assessment

In their paper (Lavanya N. *et al*., 2008) state that risk analysis is the process of identifying and analysing potential problems that could negatively impact the project, helping to avoid and mitigate the identified risks. It allows the team to be ready for any identified problems that might crop up and they can used the formulated strategy to deal with the problem and solve it. It is a very important part of Project management requirements

This section will look at some of the risks associated with the models that are going to be considered to be used for completing this project. As described earlier each model has its advantages and disadvantages, some of these disadvantages can give rise to risks threats will be explored below:

Table : The table below considers the risk involved in different Project management models Risk assessment

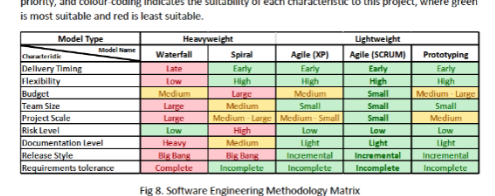
|  |  |  |  |
| --- | --- | --- | --- |
| Risk | Chance of occurring | Impact on the Project | Mitigation steps |
| One of the smaller tasks required are not completed | Low | High | Regularly check the Gantt chart to check which main task is in the process of being completed and make a requirement list for the smaller tasks present in it |
| Main DDoS datasets are too complex for the machine learning model | High | Low | Consider what columns of data is relevant to getting the results that are required. Clean the data before importing it into python. Also perform data pre-processing |
| Model chosen does not produce the result wanted | Low | High | Make changes to the model like upgrades to the steps, layers, algorithms and so on. If model cannot be adjusted then choose a new model, if time allows |
| Hardware not robust enough to perform the machine learning processing | Low | Medium | Test the machine learning model on the system being used at home, if it falls short then user the computers in the university labs. Also consider dropping data columns that are not as important for the ML model |
| The dataset does not have enough features for training a machine learning model | High | High | Research what features have been used to train ML models in previous studies. Use different method to collect data, e.g., Wireshark or tcpdump |
| Model fails to address the dates for tasks completion not being met | Low | Medium | Keep a month of time buffer from the due date of the project, if any problems arise then the model can be adjusted |
| Not enough time to finish the project before dure date | Low | High | Stick to the tasks due dates specified in the Gantt chart to complete the objectives on time |
| The model does not allow for testing and fixing bugs in the ML code | Low | Medium | Create a timeslot for testing and fixing bugs in the Gantt chart. Also contact the supervisor if any help is needed with where to find resources to fix ML code |

The risk analysis table above has brought to light some of the issues that can crop up during the duration of the process. This would allow for a predetermined plan to go into action to save time and the author would be ready if these problems came up.

## 3.1.4 Supervisor Meetings

Z

## 3.1.5 Evaluation Methodologies



Check the first dissertation for this section

**Heavyweight model(waterfall) or lightweight model (agile uses?). Scrub and Kanban are 2 models that are adaptations of the Agile model**

Table - Project management (PM) model comparison.

|  |  |  |
| --- | --- | --- |
|  | **Scrub** | **Kanban** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

Give reasons y I selected the model I did

Some awareness of project management should be demonstrated in all projects. This section should outline the nature of your project and the specific characteristics that need to be considered in determining what project management methodology you should use. You should identify the specific demands of your project in terms of project management and support your rationale for the selection of a methodology with appropriate and recent academic references. Questions which may be relevant here are:

1. What are the guiding principles and processes in managing your project?
2. What project management methods may be useful for this project?
3. How can you exploit their advantages for your project and mitigate their drawbacks?

## 3.2 Software Development

There should be a methodological analysis of software development approaches used in your project. It is important to note that what is NOT required here is a pedestrian account of popular software development methodologies or a simplistic review of their strengths and weaknesses.

Where relevant, you should give serious thought to the proper design of research and requirements capture approaches. This may include surveys, questionnaires and interviews.

## 3.3 Toolsets and Machine Environments

Toolsets refer to both software development and to project management, so the coverage should address both. This section will outline the tools for software development and project management process; it will make appropriate comparisons between tools available and argue for the most appropriate selection based on metrics, possibly a matrix diagram and other criteria. DO NOT justify the grounds for using specific toolsets and environments simply because you know them well or have developed skills already.

## 3.4 Research Methods

You should investigate the types of research methods necessary to validly answer the research questions that your project addresses. You should cite relevant sources to justify your choices.

**Chapter 4**

# Design, Development and Evaluation

3-4k words

This section of the report will vary significantly in both structure and content, depending on the type of project you are undertaking. For example, a Games design project may include a Game Design Document. However, it must be noted that if your project contains significant software development work, this should be presented in the structure expected of a formal development report. If your project involves an experimental evaluation – especially if that evaluation involved human participants – you are expected to write this work up in the format expected in Section 4.2.

## 4.1 Software Development Projects

Include this section if you are undertaking a software development project. You should discuss:

1. Requirements elicitation, gathering, collection and analysis
2. Design
3. Building and programming
4. Testing
5. Operation

## 4.2 Research Projects

If your project includes primary research components it is expected that you present this work in a manner appropriate to a scientific report:

1. Participant recruitment
2. Evidence that ethical procedures have been followed
3. Study design (short summary of research methods section) – including hypotheses/research question as appropriate
4. A detailed description of the procedure
5. Results of experiment
6. Analysis of results. Consider the results of your work with respect to both your own specific hypotheses/research question and wider context identified in your literature review.

**Chapter 5**

# Conclusions

The results from this project indicate that ...

1k words

**Chapter 6**

# Reflective Analysis

The project went well ...

1k words

# References

Alghamdie, M. (2021) Cyber security attack purpose. [image] Available from https://ars.els-cdn.com/content/image/1-s2.0-S2214785321029345-gr2.jpg [Accessed 16 November 2021]. (cit. on p. 2).

Vinayakumar, R., Alazab, M., Soman, K., Poornachandran, P., Al-Nemrat, A. and Venka-traman, S. (2019). Deep Learning Approach for Intelligent Intrusion Detection System. IEEE Access, [online] 7, pp.41525-41550. Available from https://ieeexplore-ieee-org.proxy.library.lincoln.ac.uk/stamp/stamp.jsp?tp=&arnumber=8681044&tag=1 [Accessed 23 February 2022]. (cit. on p. 6).

Musumeci, F., Fidanci, A., Paolucci, F., Cugini, F. and Tornatore, M., 2021. Machine-Learning-Enabled DDoS Attacks Detection in P4 Programmable Networks. Journal of Network and Systems Management, 30(1).

Sahoo, K., 2022. A Comprehensive Tutorial on Software Defined Network: The Driving Force for the Future Internet Technology. [image] Available from https://dl-acm-org.proxy.library.lincoln.ac.uk/doi/pdf/10.1145/2979779.2983928 [Accessed 22 May 2022]. (cit. on p. 7).

Sahoo, K., Panda, S., Sahoo, S., Sahoo, B. and Dash, R., 2019. Toward secure software-defined networks against distributed denial of service attack. The Journal of Supercomputing, 75(8), pp.4829-4874.

Alghamdie, M. (2021). A novel study of preventing the cyber security threats. Materials Today: Proceedings, [online] p.1-2. Available from https://www.sciencedirect.com/science/article/pii/S2214785321029345 [Accessed 16 No-vember 2021]. (cit. on p. 6).

Huertas Celdrán, A., Karmakar, K., Gómez Mármol, F. and Varadharajan, V. (2021). De-tecting and mitigating cyberattacks using software defined networks for integrated clinical environments. Peer-to-Peer Networking and Applications, [online] 14(5), pp.2719-2734. Available from https://link-springer-com.proxy.library.lincoln.ac.uk/article/10.1007/s12083-021-01082-w [Accessed 18 November 2021].

Kamiya, S., Kang, J., Kim, J., Milidonis, A. and Stulz, R. (2021). Risk management, firm reputation, and the impact of successful cyberattacks on target firms. Journal of Financial Economics, [online] 139(3), pp.719-749. Available from https://www.sciencedirect.com/science/article/pii/S0304405X20300143 [Accessed 16 No-vember 2021].

Liu, J., Yang, C., Chan, Y., Kristiani, E. and Jiang, W. (2021). Cyberattack detection model using deep learning in a network log system with data visualization. The Journal of Super-computing, [online] 77(10), pp.10984-11003. Available from https://link-springer-com.proxy.library.lincoln.ac.uk/article/10.1007/s11227-021-03715-6 [Accessed 17 Novem-ber 2021].

Ning, X. and Jiang, J. (2021). Design, Analysis and Implementation of a Security Assess-ment/Enhancement Platform for Cyber-Physical Systems. IEEE Transactions on Industrial Informatics, [online] 18(2), pp.1154-1164. Available from https://ieeexplore-ieee-org.proxy.library.lincoln.ac.uk/document/9444805 [Accessed 18 November 2021].

Ning, X. and Jiang, J. (2021). Functional blocks in the security enhancement module.. [im-age] Available from https://ieeexplore-ieee-org.proxy.library.lincoln.ac.uk/mediastore\_new/IEEE/content/media/9424/9594725/9444805/jiang4-3085543-small.gif [Accessed 18 November 2021].

R. Vinayakumar, M. Alazab, K. P. Soman, P. Poornachandran, A. Al-Nemrat and S. Ven-katraman (2019). Deep Learning Approach for Intelligent Intrusion Detection System. in IEEE Access, [online] vol. 7, pp. 41525-41550, Available from https://ieeexplore-ieee-org.proxy.library.lincoln.ac.uk/document/8681044/authors#authors [Accessed 18 November 2021].

Vaishali, V. (2021). Types of Cyber-attacks. [image] Available from https://d1m75rqqgidzqn.cloudfront.net/2019/10/26-september-cyber-security-attack-infographic-1.jpg [Accessed 18 November 2021].

Yang, C., Kristiani, E., Wang, Y., Min, G., Lai, C. and Jiang, W. (2019). On construction of a network log management system using ELK Stack with Ceph. The Journal of Supercom-puting, [online] 76(8), pp.6344-6360. Available from https://link-springer-com.proxy.library.lincoln.ac.uk/article/10.1007%2Fs11227-019-02853-2 [Accessed 18 No-vember 2021].

NeuralNine. (2019). *Code A DDOS Script In Python - NeuralNine*. [online] Available from <https://www.neuralnine.com/code-a-ddos-script-in-python/> [Accessed 21 May 2022].

CloudFlare. (2022). *What is a DDoS attack?*. [online] Available from https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/ [Accessed 21 May 2022].

Kerzner, H. (2003\_. *Project management workbook*. Hoboken, N.J.: Wiley, p.4. (cit. on p. 10).

Friedman, J., 2020. *5 Phases of Project Management*. [image] Available from https://www.truenxus.com/blog/five-phases-of-project-management [Accessed 23 May 2022]. (cit. on p. 11).

Cohen, E. (2022). The Definitive Guide to Project Management Methodologies. [Blog] *workamajig*, Available from https://www.workamajig.com/blog/project-management-methodologies [Accessed 23 May 2022].

Cohen, E., (2022). *The Definitive Guide to Project Management Methodologies*. [image] Available from https://www.workamajig.com/blog/project-management-methodologies [Accessed 23 May 2022]. (cit. on p. 11, 12).

Lavanya, N. and Malarvizhi, T. (2008). Risk Analysis And Management. [online] Pmi.org. Available from https://www.pmi.org/learning/library/risk-analysis project management-7070 [Accessed 24 May 2022]

University of Lincoln (2020) Referencing Handbook: Harvard. Lincoln: University of Lincoln.

# Word Count

XXXX