

Department of Electronic & Electrical Engineering

MEng/BEng in EEE

19496 Individual Project

This document is organised in to six parts:

PART 1: STATEMENT OF INTENT
PART 2: PROJECT WORK PLAN
PART 3: RESOURCE REQUIREMENTS
PART 4: RISK ASSESSMENT
PART 5: SUSTAINABILITY, ETHICS, INCLUSIVITY
PART 6: SAFETY DECLARATION & ETHICS APPROVAL

- All parts of the form must be completed jointly by the student and Project Supervisor, and lodged (by the student) on MyPlace by **14.00 on 14 October 2022**.
- Copies of the completed form should be sent to the Project Supervisor.
- The student is advised to retain a copy of the completed form for future reference - ideally affixed inside their project logbook.
- Students will be asked to reflect upon parts 1, 2 and 4 at the interim stage and also in the final report.

Supervisor's Name: Dr Robert Atkinson	Student's Name: Julien Priam
Project Title: AI (Machine Learning) for Cyber Security using Limited Data	

PART 1: STATEMENT OF INTENT

The purpose of this section is: (i) to provide a concise description of the project, and (ii) to state a set of objectives that will provide the guide for assessing the project. Students should note the importance of item (ii), which should be discussed in detail with their project supervisors.

A. Project Description:

The student, in consultation with the Project Supervisor, is required to describe the project in THEIR OWN WORDS in the space provided below (in about 200 to 300 words). Note that simply copying descriptions in the project listing is unacceptable. THIS PART SHOULD NOT BE COMPLETED BY THE PROJECT SUPERVISOR other than ensuring the accuracy of the description. DO NOT ATTACH EXTRA PAGES.

With the incredible growth of the internet during the last decades, more and more data are stocked and shared online. These raises are huge issues for people to keep their information secret, against cyber attackers who develop always more sophisticated malwares.

In an objective to detect and counter these attacks, intrusion detection systems are developed, some of them using Machine Learning. This project aims to develop one of these systems with different machine-learning approaches. To begin with, a first artificial intelligence (AI) model will be developed using Python and useful libraries such as Panda, Keras... In order to train the AI, we will use a dataset (CICIDS2017) containing network traffic captures for five days a week. The dataset regroups different types of attacks such as Brute Force FTP, Brute Force SSH, DoS, Heartbleed, Web Attack, Infiltration, Botnet, and DDoS.

However, such AI are often hard to train due to the lack of datasets related to the subject. That is why the project will then be about improving the AI to be trained using limited data.

B. Project Objectives:

Project objectives must be stated in such a way that they can be translated into achievable goals during the conduct of the project. For this reason, the stated objectives must be specific and realistic to be attained within the time provided. It will be very helpful if supervisors encourage their students to come up with initial objectives from students' perspective as this exercise could help students to better understand the aims of the project. It is important to note that the achievements of the project work will be measured against the objectives stated here. Copies of this section will be made available to persons involved with the assessment of this project.

1. Under the "Importance" column below, enter one of the following as appropriate: "Major", "Minor", or "Optional".
2. If at a later stage, the project objectives change significantly, these changes must be communicated clearly in the interim and final report as appropriate.

Project Objectives	Importance
Parse Dataset (pcap files) and store relevant information in a dataframe	Major
Test different Machine Learning models to train an AI	Major
Obtain a functional Machine Learning algorithm with a large dataset	Major
Obtain a functional Machine Learning algorithm on a small dataset	Major

PART 2: PROJECT WORK PLAN

Identify project milestones and summarise your work plans in the table below in the order you do them.
(Example: preliminary design, prototyping, simulation modelling, results validation, write-up, etc.).

	Project Milestones/Work Phases	Expected Week Time Enter start and end week Ex.: Week 6 to week 8
1	Set up a work environment on computer	Week 2 to week 3 (S1)
2	Statement of Intent	Week 3 to week 4 (S1)
3	First Python script which parses pcap files, extracting relevant information	Week 3 to week 4 (S1)
4	Determine the best features to work on with a simple Machine Learning model	Week 4 to week 5 (S1)
5	Test different Machine learning model <ul style="list-style-type: none">• Linear regression• Decision tree• Random forest• SVM classifier	Week 5 to week 7 (S1)
6	Work on the selected Machine Learning model	Week 7 to week 11 (S1)
7	Interim assessment	December (S1)
8	Improvement of AI to be trained using limited data	Week 1 to week 9 (S2)

9	Oral examination	Week 0 (S2)
10	Poster presentation	Week 11 (S2)
11	Final report	Week 11 (S2)

PART 3: RESOURCE REQUIREMENTS

A. Software:

List the software required for the project. This includes programming languages, application packages, CAD tools, etc.

Software (indicate version no. if applicable)	Software Administrator (EEE/MAE/CIS Dept, Comp. Centre)	Installed Location (Dept/Central University/ Personal computer).	Expected Usage (hours/week)
Python 3.10	Me	Personal computer	10h/w
PyCharm (Python IDE 2022.2.2)	Me	Personal computer	10h/w
Oracle VirtualBox 6.1	Me	Personal computer	10h/w

B. Hardware:

List major hardware components such as circuit boards, microcontrollers, LSI/VLSI integrated circuits, and special purpose equipment and facilities.

No hardware required for this project

C. Background Information & Required Reading

<i>Describe sources of information (in library and elsewhere) required to undertake project</i>
<ol style="list-style-type: none"> 1. "Python Machine Learning - Third Edition" - Sebastian Raschka, Vahid Mirjalili 2. Wikipedia (Pandas, dpkt, keras, sklearn...) 3. "A taxonomy of malicious traffic for intrusion detection" - Dr Robert Atkinson 4. "The Curse of Dimensionality: Inside Out" - Naveen Venkat
<i>Provide details of the two most important sources of information already identified</i>
<ol style="list-style-type: none"> 1. This book is a step-by-step tutorial to build a first Machine learning system. It contains illustrations and a lot of working examples. The models are based on Keras library. 2. Wikipedia is a useful source of information, covering most of the thematic covered in this project. It is a good start to get familiar with specific notions or libraries

D. Laboratory/Work Area:

<i>Indicate the laboratory room(s) and/or project work area for the project.</i>
<ul style="list-style-type: none"> • Personal desk • Strathclyde library

With regards to practical work there is no expectation/requirement that practical work on the project is carried out anywhere other than on University campus. Any work that is carried out off-site must be fully agreed by supervisor and explicitly covered by the project's risk assessment – and listed in the space provided below.

D. Logbook:

Confirmation that student has A4, hardback, bound logbook that has been viewed by the supervisor and/or arrangements have been made for shared access for electronic logbook/progress records. (Teams/OneNote recommended) YES

PART 4: TECHNICAL RISK

Management of project work requires that technical risk be assessed in advance, during initial planning and as an ongoing process. As the first stage to this process, identify any aspects of risk associated with your project proposal. Risk in this context is taken to mean any event or action (or inaction) that would jeopardise any project outcomes or significantly impede project progress. Furthermore, having identified such potential risks, indicate what actions you would take to mitigate the effects of this risk. (Consult your supervisor for advice but examples of such risks include non-delivery of a key component, illness or absence from University, non-completion by student or other of key deliverable, equipment malfunction, extended learning curves-new techniques or software, etc.).

	Possible Risk:	Mitigating Action:
1	Back pains	Work on adjustable desk chair
2	Eyes trouble	anti-blue light glasses.
3	Computing power	Use tools such as google colab or ask for an university computer
4	Insufficient internet connection (no ethernet port on computer)	Work on the campus during lull periods
5		

PART 5: SUSTAINABILITY, ETHICS AND INCLUSIVITY

All project students will in the course of their work implement and develop technological advancements, either through the creation of prototypes, software tools and or generation of new know-how/ways of doing things. The focus of such development is typically aligned to a combination of technological, societal or financial drivers.

As major drivers of technology advancement, engineers have key role in stewardship of the planet's resources. Sustainability could be demonstrated by comparing the developments, techniques and ideas that encompass the project and making comparison to status quo, how resources can be saved/reserved etc. Furthermore, new developments to address current needs should not negatively impact the ability of future generations to meet and address their own needs. How would that be achieved/developed in the course of the project?

Ethics form an essential part of engineering practise and ensure that project teams and persons affected by project outcomes are all treated fairly, equally, openly and with integrity. These ethical standards can be considered and applied to the different phases of the project: planning; sourcing and utilisation of project inputs (data, raw materials, components etc.); milestones/decision points through the course of the project; implementation of the final deliverable(s); manufacturing; safety implications, both during the course of the project and in utilisation of any final deliverable.

Engineering and technology are for everyone and technological solutions to the many challenges we face as a society should encompass and benefit all members of society irrespective of age, gender, race, ability or socio-economic standing.

In considering your project, describe how aspects of sustainability, ethics and inclusivity have been considered and impacted the project and its outcomes. The Sol can be used to capture how such factors have influenced the initial planning of the project and subsequent reports, both interim and final, can be used to record how such factors have influenced the course of the project, deliverables, milestones, and outcomes.

Artificial intelligence generally requires enormous computing power, which implies high electricity consumption. As engineers, we need to think about this impact on the environment and do everything we can to reduce it. This includes paying particular attention to code writing in order to minimise the calculations carried out.

From an ethical point of view, we work with large amounts of data, so it is important to ensure confidentiality.

PART 6: SAFETY DECLARATION & ETHICS APPROVAL

SAFETY DECLARATION

All project students must be aware of the need for safe working during the conduct of their project. The Area Safety Regulations for the Department of Electronic and Electrical Engineering, which appear in the Project and Course MyPlace pages and provide general guidance. Project students should consult with their Supervisor to obtain specific instructions or written additional Risk Assessment relating to their own project.

By signing at the end of this form, the project student is declaring that they have:

1. attended the EEE UG Individual Project safety seminar.
2. completed the online safety assessment quiz
3. read and understood the Area Safety Regulations and will abide by these regulations during the conduct of the project, and
4. consulted with the Project Supervisor who, if applicable, has specified any additional Risk Assessment or additional Safe Systems of Work and Standard Operating Procedures. These need to be specified in a risk assessment completed and uploaded to the University's eRisk server.

<https://safetystrath.ac.uk/> in due course.

Location	(Provide a summary of intended additional risk assessments. Enter NONE if not applicable)
	NONE

ETHICS APPROVAL

Please indicate below if the project may require ethics approval. Approval will be required if the project will utilise or generate personal data obtained directly from individuals (interviews, surveys, on-site measurements) or use clinical or personal data obtained from a 3rd party. The supervisor has ultimate responsibility to identify and then obtain appropriate ethics approval and the project will not progress (in this area) until such approval is granted.

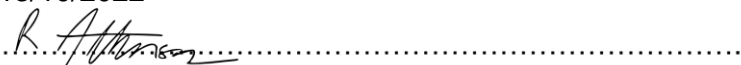
Summarise below where/why ethics approval may be sought and when will be applied for	Approved
	Y/N

Signature of Student



Date 13/10/2022

Signature of Supervisor



...13/10/22.....