Cyber-Events Detection tool within a Smart Grid to increase Situational Awareness

Initial plan Template

CARDIFF UNIVERSITY SCHOOL OF INFORMATICS

INITIAL PLAN

CM3203 - ONE SEMESTER INDIVIDUAL PROJECT

AUTHOR: KYLE SWIRE-THOMPSON

SUPERVISOR: NEETESH SAXENA

MODERATOR: HANTO LIU

Project Description

The project aims to develop cyber events detection capability in the smart grid for improving situational awareness. The work involves finding the indicators of compromise, packet analysis, and exploring other footprints to understand the nature of the events and cyber-behaviour. Within the context of this project, there are different terms which need to be defined there are three elements to this project that need to be defined these are: a cyber event, A smart grid and Situational awareness. a cyber event is an occurrence in an information system and or network that has or can result in the corruption or unauthorized access, processing, modification, transfer, or disclosure of data and/or Confidential Information in the context of an attack there are three main types of attacks which are then divided into different sub-category's these are Data Injection, Remote Tripping Command Injection and Relay Setting Change. A cyber event may also be a planned event like one or more relays being disabled to do maintenance for that relay/relays. A smart grid is an electrical grid with automation, networking, communication, and IT systems as well as other computerized elements. It is used to control the transition of energy from generation plants to users while improving efficiency, quality's and safely of the overall system. Finally, Situational awareness of a smart grid is the use of advanced monitoring technology to understand and develop an idea of what is happening in a smart grid to recognize an abnormal event.

❖ Why this tool matters?

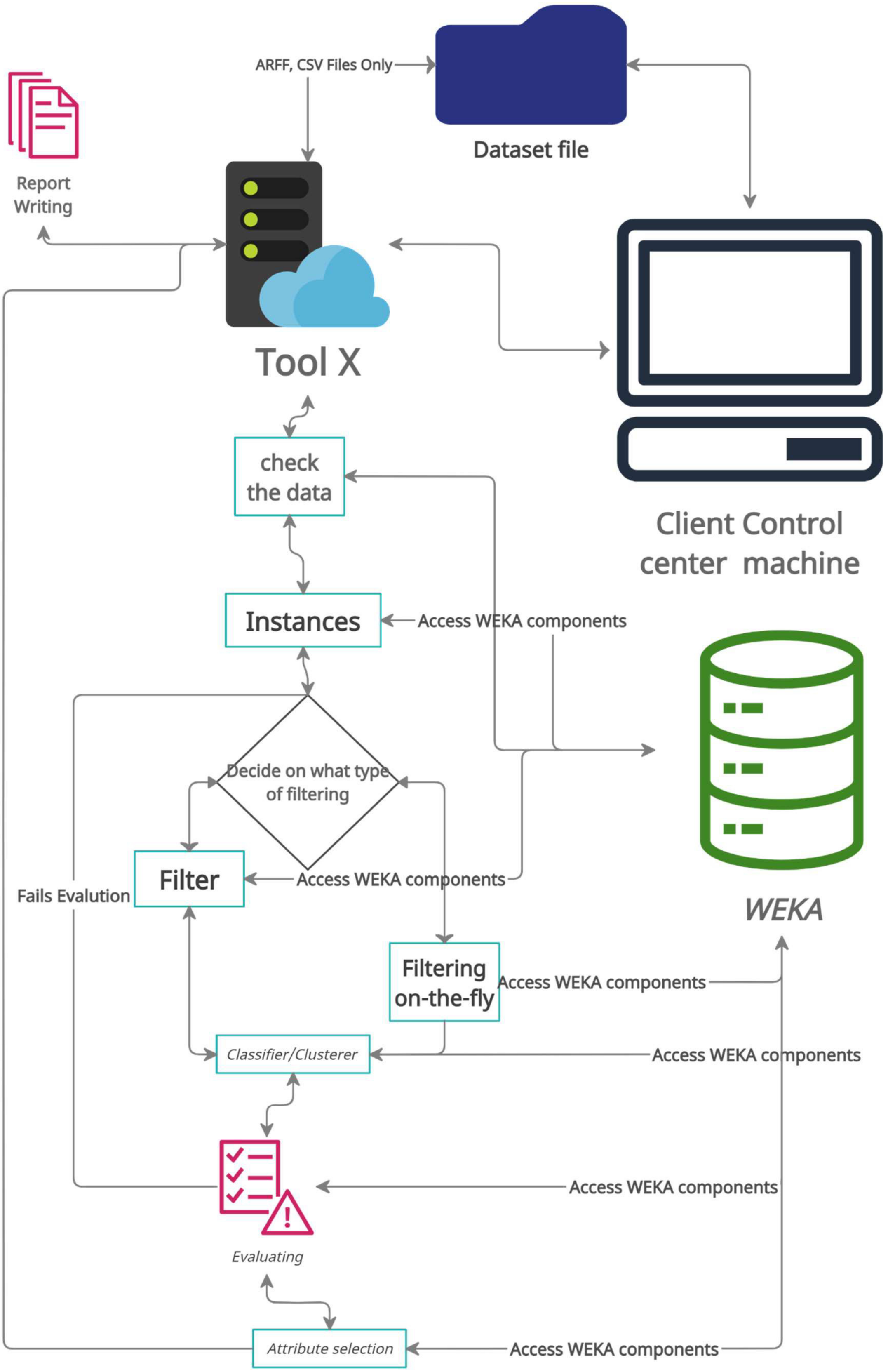
- this tool is trying to solve the problem of recognition and classification of different cyber events to improve the response of the first responders. The tool will then produce a report on any flagged events, which a first responder can use to gain a better understanding of the events that occurred and respond or effectively if the situation requires it.

- In December of 2015, the Ukrainian power grid was attacked and disrupted the services of nearly 250,000 people. This is thought to be a test run which then can be used as portions of a larger offensive, military or otherwise [1]. Some security experts warn that this type of event is easily scalable to grids elsewhere [2].

- The Insurance company Lloyd's of London modelled the outcome of a potential cyberattack on the Eastern Interconnection, which is one of the two major alternating-current (AC) electrical grids in the continental U.S. power transmission grid, which has the potential to impact 15 states, put 93 million people in the dark, and could cost the country's economy anywhere from $243 billion to $1 trillion in various damages [3].

❖ what the Tool will do

- ➢ My product will be constantly running in the control centre and will be used to monitor data through different files that the tool will fetch and check for any abnormal cyber events. Using the WEKA tool as the machine learning aspects I will use it to read through each dataset and find any abnormalities which may pertain to a cyber event or any event which should be reported on to the system admin. Once a report has been created for each occurrent of an events error then be passed on to the system admin for the relevant first responder with the correct permissions. If there is no abnormal event detected within the data sets provided the tool with wait for a new file to analyses.



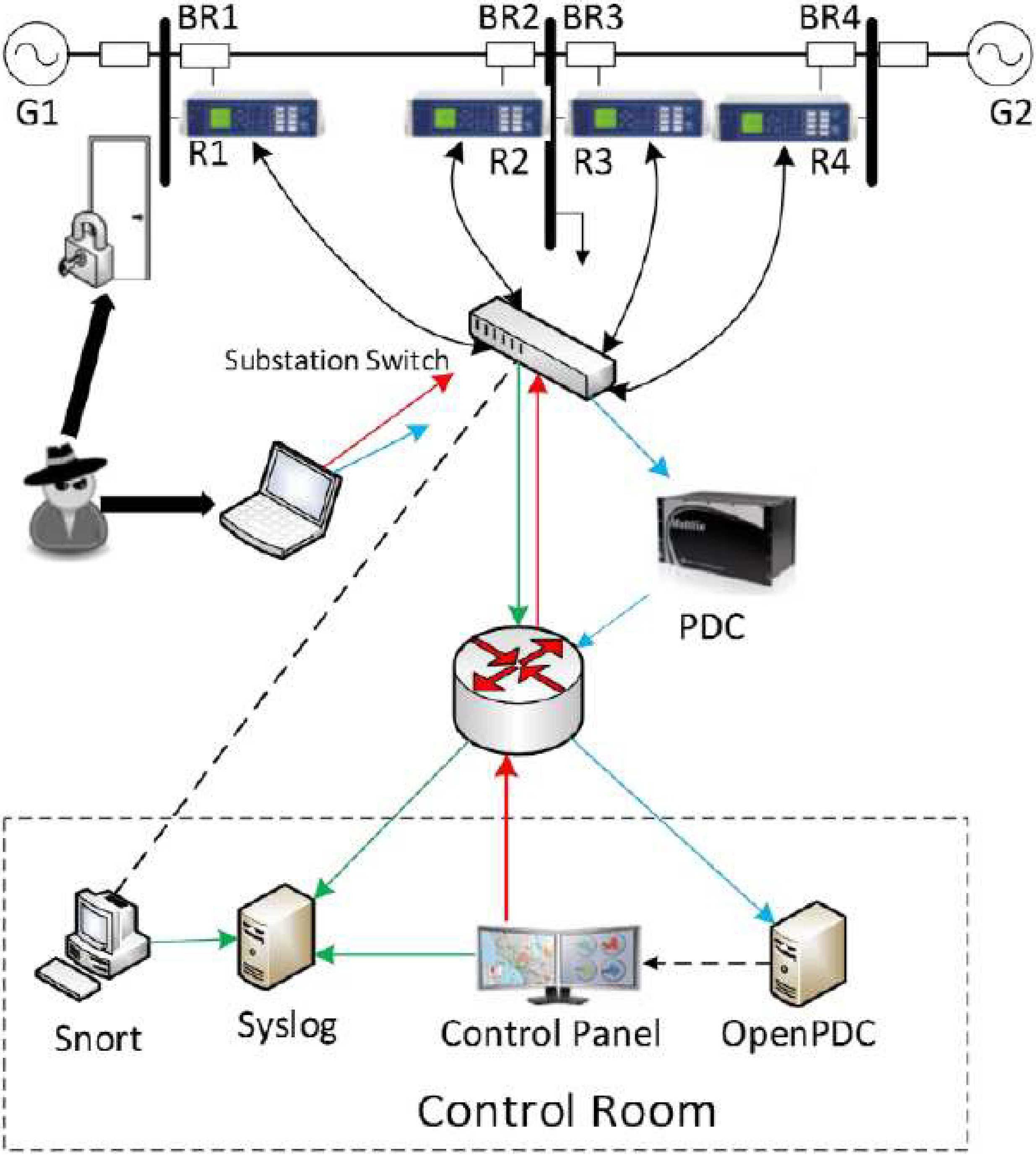
TOOL X DIAGRAM

Note:

the dataset file, client control centre machine and WEKA Tool are not controlled by the user. Tool x and the data set file are controlled by the client control centre machine whereas WEKA is a Waikato Environment for Knowledge Analysis, developed at the University of Waikato, New Zealand.

❖ Diagram of how my tool will fit into the smart grid system

- The figure below shows the power system framework configuration used in generating these scenarios.



Project Aims and Objectives

- *Project Aim*
  - *The overall aim of the project is to implement a tool that will improve the situational awareness of a first responder in regards to any cyber events that were to occur on the smart grid, this will involve using machine learning on collected data to find any abnormal events that may occur.*
- *Objective 1*
  - *Retrieve smart grid data and translate it into a format that can be read by a machine learning tool.*
- *Objective 2*
  - *Implement a methodology and machine learning tool on the translated data to recognize abnormal activity which may constitute an attack.*
- *Objective 3*
  - *if the cyber event is recognized to be an attack then a clear and concise report must be created for the first responder to easily be able to understand the situation and react in a fast and effective manner, reducing the impact of the attack on the smart grid.*

Ethics

- Data privacy
  - I have 3 datasets which include measurements related to electric transmission system normal, disturbance, control, cyber-attack behaviours all created without personal data being used.
  - Originally developed by Uttam Adhikari, Shengyi Pan, and Tommy Morris in collaboration with Raymond Borges and Justin Beaver of Oak Ridge National Laboratories (ORNL)
- Anonymity
  - The data I will be using does not involve human participation therefor anonymity is not a problem.
- intellectual-property
  - if the correct academics, academic institutions and any other sources of information or help are correctly recorded and sighted then there won't be a problem
  - I will be following the Cardiff University research integrity and governance code of practice version 3 if an issue arises or I am unsure as to what the correct procedure should be
- Cardiff University's Research Ethics Committee
  - Procedure and Forms
    - Using the Procedure and Forms I can see that there is no need for an ethical approval procedure

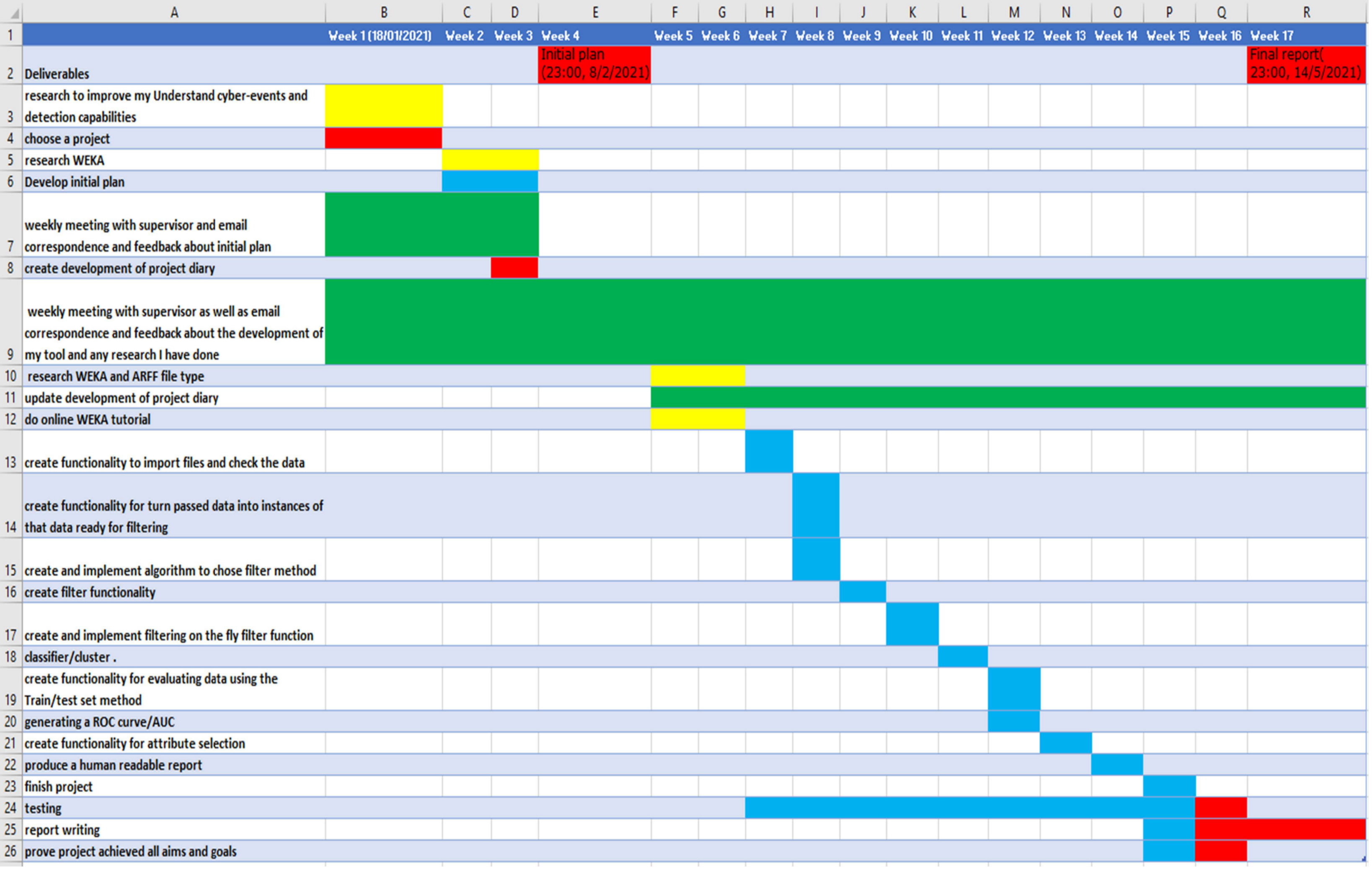
Work Plan

Here I will include a week by week break down off what I will be doing, researching, any communications with my supervisors, any goals I have achieved and if anything is to be handed in.

- Week 1 (Mon 18/01/2021) – research to improve my Understand cyber-events and detection capabilities from previous literature and open source tools, choose a project
- Week 2 (Mon 25/01/2021) - research WEKA, Develop initial plan, weekly meeting with supervisor and email correspondence and feedback about the initial plan
- Week 3 (Mon 01/01/2021) - research WEKA, Develop and finish initial plan, weekly meeting with supervisor and email correspondence and feedback about the initial plan
    - Hand in the initial plan submitted by 23:00, 8/2/2021
- Week 4 (Mon 08/02/2021) - weekly meeting with the supervisor as well as email correspondence and feedback about the development of my tool and any research I have done (this will now be referred to as "recurring weekly meeting"), create and update development of project diary
- Week 5 (Mon 15/02/2021) - recurring weekly meeting, research WEKA and ARFF file type, complete first half of online WEKA tutorial, update development of project diary
- Week 6 (Mon 22/02/2021) - recurring weekly meeting, research WEKA and ARFF file type, complete second half of online WEKA tutorial, update development of project diary
- Week 7 (Mon 01/03/2021) - recurring weekly meeting, create functionality to import files and check the data is correct if not convert into the required format, update development of project diary
- Week 8 (Mon 08/03/2021) - recurring weekly meeting, create functionality for turn passed data into instances of that data ready for filtering, create and implement an algorithm to chose filter method. update development of project diary
- Week 9 (Mon 15/03/2021) - recurring weekly meeting, create filter functionality via implementing the OptionHandler interface, update development of project diary
- Week 10 (Mon 22/03/2021) - recurring weekly meeting, create and implement filtering on the fly filter function, update development of project diary
- Week 11 (Mon 29/03/2021) - recurring weekly meeting, classifier/cluster. here I will choose the best methodology to handle the data that has been filtered, these options are classifier or cluster, a combination of both may even be possible but I will research into this, update development of project diary

- Week 12 (Mon 05/04/2021) - recurring weekly meeting, create functionality for evaluating data using the Train/test set method, if possible, generating a ROC curve/AUC if time allows, update development of project diary
- Week 13 (Mon 12/04/2021) - recurring weekly meeting, create functionality for attribute selection using meta-classifier, filter and low-level, update development of project diary
- Week 14 (Mon 19/04/2021) - recurring weekly meeting, write a program that will produce a human-readable report to be passed to the first responder based on the results from all the data processing, update development of project diary
- Week 15 (Mon 26/04/2021) – recurring weekly meeting, finish the project, complete testing phase of code, start writing the report, update development of project diary
- Week 16 (Mon 03/05/2021) – recurring weekly meeting, further testing to prove project achieved all aims and goals, report writing, update development of project diary
- Week 17 (Mon 10/05/2021) – recurring weekly meeting, final checks on project report and code
    - Hand in Final report and code submit by 23:00, 14/5/2021

Gantt chart



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
1		Week 1 (18/01/2021)	Week 2	Week 3	Week 4	Week 5	Week 6	Week 7	Week 8	Week 9	Week 10	Week 11	Week 12	Week 13	Week 14	Week 15	Week 16	Week 17
2	Deliverables				🟥 Initial plan (23:00, 8/2/2021)													🟥 Final report(23:00, 14/5/2021)
3	research to improve my Understand cyber-events and detection capabilities	🟨																
4	choose a project	🟥																
5	research WEKA		🟨	🟨														
6	Develop initial plan		🟦	🟦														
7	weekly meeting with supervisor and email correspondence and feedback about initial plan	🟩	🟩	🟩														
8	create development of project diary			🟥														
9	weekly meeting with supervisor as well as email correspondence and feedback about the development of my tool and any research I have done	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
10	research WEKA and ARFF file type					🟨	🟨											
11	update development of project diary					🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
12	do online WEKA tutorial					🟨	🟨											
13	create functionality to import files and check the data							🟦										
14	create functionality for turn passed data into instances of that data ready for filtering								🟦									
15	create and implement algorithm to chose filter method								🟦									
16	create filter functionality									🟦								
17	create and implement filtering on the fly filter function										🟦							
18	classifier/cluster .											🟦						
19	create functionality for evaluating data using the Train/test set method												🟦					
20	generating a ROC curve/AUC												🟦					
21	create functionality for attribute selection													🟦				
22	produce a human readable report														🟦			
23	finish project															🟦		
24	testing							🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟥	
25	report writing															🟦	🟥	🟥
26	prove project achieved all aims and goals															🟦	🟥	

References

[1] Knake, Robert. "A Cyberattack on the U.S. Power Grid". Council on Foreign Relations. Retrieved 2017-10-22.

[2] "'Crash Override': The Malware That Took Down a Power Grid". WIRED. Retrieved 2017-10-19.

[3] "New Lloyd's study highlights wide-ranging implications of cyber attacks". www.lloyds.com. 8 July 2015. Retrieved 2017-10-22.