MSE | MASTER OF SCIENCE IN ENGINEERING

Hes·so
Haute Ecole Spécialisée de Suisse occidentale
Fachhochschule Westschweiz
University of Applied Sciences and Arts Western Switzerland

Master of Science HES-SO in Engineering
Av. de Provence 6
CH-1007 Lausanne

Master of Science HES-SO in Engineering

Orientation: Information and Communication Technologies (ICT)

Provide Secured Environment for AI Projects
Specification document

Author
Loïc GUIBERT

Under the direction of
Dr. Pascal BRUEGGER
HES-SO//Master, iCoSys
and
Dr. Adriana WILDE
University of Winchester, WINTS

Winchester, HES-SO//Master, 29th September 2022

Contents

List of Figures

1 Introduction

This specifications document describes all the elements necessary to understand the characteristics of the Master Thesis that takes place in the *HES-SO//Master* curriculum.

A Master thesis takes place at the end of all the Master lectures during a whole semester. An amount of nine hundred hours must be dedicated to this end and at least one weekly meeting must be organized through the whole project duration.

This thesis will be realized in collaboration between the *HES-SO//Master* and the *University of Winchester*. The student will realize his thesis abroad, at the city of Winchester.

In this document will be explained the context, objectives, activities and planning of the thesis.

All the documents produced during this project will be stored on the School of Engineering and Architecture of Fribourg (HEIA-fr) software forge[1].

2 Context

This chapter will describe the context around the subject of the thesis. We will explain the actual state that contains a problem to be solved, and the author's contribution that will contribute to fix the previously described problem. We will also introduce the different actors that will intervene during the thesis.

2.1 Actual State

In a world where Informational Technologies (IT) security is increasingly valuable and necessary, the need for new ways to secure and trust information systems is growing. This need is particularly expressed in the Artificial Intelligence (AI) field, where big amounts of data are periodically collected in order to improve services performances or to monetize them. Furthermore, such data is often personal and highly related to their user, which raise ethical and privacy-related questions.

Nowadays, end users of public or private online services are more and more aware of personal data related risks and a change in consumption patterns is being noticed. Therefore, new approaches for the whole IT field must be developed in order to provide secured and privacy-first online services that can nevertheless enable a personalized experience.

2.2 Contribution

By enabling secured and privacy-oriented personalized experience on online services, companies would be able to provide ethical, modern and respectful offers to their customers. All stakeholders would benefit from such implementations, as long as the performance, time or processing capabilities do not restraint them in their activities.

This thesis aims to provide which technologies, best practices or safeguards can be integrated to information systems in order to ensure secured environments to the end users, particularly regarding AI projects. These components must then be implemented in a functional information system, which includes AI processes, while providing a conclusion on the changes of such integration compared to the initial information system.

We want to offer a suitable solution to those wishing to increase the security and confidentiality of their online services. A focus will also be made on the AI field.

2.3 Actors

The thesis will be conducted by Loïc Guibert.

There are two advisors for this thesis: Dr. Pascal Bruegger and Dr. Adriana Wilde.

The thesis subject has been proposed by Loïc Guibert as a personal project and is related to the field of research of the two advisors. A secured online service is being developed by Dr. Pascal Bruegger and includes aspects similar to this thesis subject.

An expert will be assigned to the thesis in order to evaluate it when completed and returned. This assignment will be made later during the semester.

3 Objectives

Following the enumeration made in 2.2 (Contribution), questions need to be asked in order to complete this project.

- Which rules, best practices, technologies and aspects should be used in order to improve the security and confidentiality of online services?
- Which specific rules, best practices, technologies and aspects should be used in order to improve the security and confidentiality of the AI field, particularly for Machine Learning (ML) and Deep Learning (DL) models?
- How can we provide an understandable and complete model of our findings?

The objectives below intent to provide answers to the questions asked.

3.1 Primary Objectives

All those objectives must be fulfilled in order to successfully complete the thesis.

3.1.1 Establish an Up-To-Date Knowledge Collection

We need to collect an up-to-date and complete knowledge of the rules, best practices, technologies and aspects that contribute to enforce the security and privacy of online services. To this end, a proper literature review must be conducted. Its results will then be used as a foundation for the next phase of the thesis.

The content related to this objective must be included into the thesis report. It will list, explain and analyse the concepts found during the collection.

This objective must be completed before the end of the thesis, which is the 10th February 2023.

3.1.2 Provide an Understandable Guide or Framework

Using the previously collected knowledge about security and privacy, a guide or framework must be built. It must provide an understandable and appliable methodology in order to evaluate online services.

The content related to this objective must be included into the thesis report. It will list, explain and analyse the methodology used to build the guide or framework and its content. The result of this objective will be an independent document, which must be attached to the thesis report as an appendix.

This objective must be completed before the end of the thesis, which is the 10th February 2023.

3.1.3 Apply and Test the Guide or Framework on an Online Service

Proper metrics must be used in order to conduct a proper evaluation of the guide or framework. Once defined and explained, an evaluation of an online service including one or more AI processes will be made, and the results will then be analysed and discussed.

The online service should be accessible and open, which means that we should have access to the source code. To this end, we could use the *Hestia*[1] ecosystem, which is an ongoing project leaded by Dr. Pascal Bruegger.

The content related to this objective must be included into the thesis report. It will explain and analyse the results obtained during the evaluation.

This objective must be completed before the end of the thesis, which is the 10th February 2023.

3.2 Secondary Objectives

The secondary objective will only be completed if all primary objectives have been fulfilled and if there is still time left before the end of the project's timeframe.

3.2.1 Submit the Guide as an Online Resource

Because of the nature of this thesis being an academical work and the ethics of such approaches, we believe that publishing the guide or framework on the Internet would be useful to the public. It should therefore be published on some online platforms, such as a custom website, a forum or something equivalent.

The content related to this objective must be included into the thesis report. It will explain and analyse the approaches made in order to publish the guide or framework online.

If this objective is considered, it must be completed before the end of the thesis, which is the 10th February 2023.

3.3 Constraints

Apart from the ones described in the respective objectives, an additional constraint must be respected regarding the whole thesis scope.

If any data collected under real-life conditions is used, analysed or processed during this thesis, ethical considerations and obligations must be applied.

[1] *Hestia* source: `https://bit.ly/3BzeDSN` (accessed 22nd September 2022)

4 Activities

The previously defined objectives imply several work activities in order to fulfil them. These activities are separated into more specific tasks. Please note that those tasks will not necessarily be done in a chronological order.

4.1 Specifications

This activity defines the scope and objectives of the thesis.

1. Define the project specification
2. Define the project planning

4.2 State of the Art

This activity covers the 3.1.1 (Establish an Up-To-Date Knowledge Collection) objective.

1. Gather scientific articles and papers
2. Gather online resources
3. Gather standards
4. Gather technologies
5. Assess, analyse and explain the relevant resources

4.3 Methodology

This activity partially covers the 3.1.2 (Provide an Understandable Guide or Framework) objective.

1. Define and explain the guide or framework chosen format
2. Gather resources for the chosen format
3. Prepare the document

4.4 Build the Guide or Framework

This activity partially covers the 3.1.2 (Provide an Understandable Guide or Framework) objective.

1. Define the categories
2. Define the items to evaluate
3. Define the evaluation process

4.5 Test and Evaluation

This activity covers the 3.1.3 (Apply and Test the Guide or Framework on an Online Service) objective.

1. Define the proper metrics to evaluate the guide of framework
2. Get access to an online service
3. Apply the methodology previously defined
4. Evaluate and explain the results

4.6 Publish the Guide or Framework

This activity covers the 3.2.1 (Submit the Guide as an Online Resource) secondary objective.

1. Assess the suitable online platforms
2. Publish the document on selected platform(s).

4.7 Documentation

The thesis report will be realized throughout the duration of the whole project, but this activity will be conducted at its end in order to change last details in said report. A poster must also be produced.

1. Produce the thesis poster
2. Finalize the thesis report

5 Planning

Around nine hundred hours of work are required for this thesis: this amount depends on the number of indicated credits.

The public holidays are taken into account: one week of break has been planned during winter holidays. Weekends are not included into the planning but can be used to catch up possible delays.

We will work with the Scrum method, which is an iterative agile method. The duration of the sprints is of one week excepted for exceptions due to special occasions (sprints number 1, 13, 14 and 18), with a backlog definition made at each weekly meeting. The tasks defined in 4 (Activities) can be directly included into the backlog or can be divided into smaller tasks.

The major observed differences will be notified into meeting minutes.

Figure 5.1 (Gantt planning of the thesis) shows a graphical view of the corresponding planning.

5.1 First Sprint (1st)

Timeline:

- Start - 19.09.2022
- End - 28.09.2022

Activity to complete:

- 4.1 (Specifications)

Deliverable:

- Specifications document

5.2 Second Sprint (2nd)

Timeline:

- Start - 29.09.2022
- End - 05.10.2022

Activity to complete:

- 4.2 (State of the Art)

Deliverable: none

5.3 Third Sprint (3rd)

Timeline:

- Start - 06.10.2022
- End - 12.10.2022

Activity to complete:

- 4.2 (State of the Art)

Deliverable: none

5.4 Fourth Sprint (4th)

Timeline:

- Start - 13.10.2022
- End - 19.10.2022

Activity to complete:

- 4.2 (State of the Art)

Deliverable: none

5.5 Fifth Sprint (5th)

Timeline:

- Start - 20.10.2022
- End - 26.10.2022

Activity to complete:

- 4.2 (State of the Art)

Deliverable: none

5.6 Sixth Sprint (6th)

Timeline:

- Start - 27.10.2022
- End - 02.11.2022

Activity to complete:

- 4.2 (State of the Art)

Deliverable: none

5.7 Seventh Sprint (7th)

Timeline:

- Start - 03.11.2022
- End - 09.11.2022

Activity to complete:

- 4.2 (State of the Art)

Deliverables:

- An up-to-date state of the art
- Report content

5.8 Eighth Sprint (8th)

Timeline:

- Start - 10.11.2022
- End - 16.11.2022

Activity to complete:

- 4.3 (Methodology)

Deliverable: none

5.9 Ninth Sprint (9th)

Timeline:

- Start - 17.11.2022
- End - 23.11.2022

Activity to complete:

- 4.3 (Methodology)

Deliverables:

- Defined methodology for the guide or framework
- Report content

5.10 Tenth Sprint (10th)

Timeline:

- Start - 24.11.2022
- End - 30.11.2022

Activity to complete:

- 4.4 (Build the Guide or Framework)

Deliverable: none

5.11 Eleventh Sprint (11th)

Timeline:

- Start - 01.12.2022
- End - 07.12.2022

Activity to complete:

- 4.4 (Build the Guide or Framework)

Deliverable: none

5.12 Twelfth Sprint (12th)

Timeline:

- Start - 08.12.2022
- End - 14.12.2022

Activity to complete:

- 4.4 (Build the Guide or Framework)

Deliverable: none

5.13 Thirteenth Sprint (13th)

Timeline:

- Start - 15.12.2022
- End - 23.12.2022

Activity to complete:

- 4.4 (Build the Guide or Framework)

Deliverable: none

Winter vacations

5.14 Fourteenth Sprint (14th)

Timeline:

- Start - 02.01.2023
- End - 11.01.2023

Activities to complete:

- 4.4 (Build the Guide or Framework)
- 4.5 (Test and Evaluation)

Deliverables:

- Guide or framework
- Report content

5.15 Fifteenth Sprint (15th)

Timeline:

- Start - 12.01.2023
- End - 18.01.2023

Activity to complete:

- 4.5 (Test and Evaluation)

Deliverable: none

5.16 Sixteenth Sprint (16th)

Timeline:

- Start - 19.01.2023
- End - 25.01.2023

Activity to complete:

- 4.5 (Test and Evaluation)

Deliverable: none

5.17 Seventeenth Sprint (17th)

Timeline:

- Start - 26.01.2023
- End - 01.02.2023

Activity to complete:

- 4.5 (Test and Evaluation)

Deliverable: none

5.18 Eighteenth Sprint (18th)

Timeline:

- Start - 02.02.2023
- End - 08.02.2023

Activity to complete:

- 4.5 (Test and Evaluation)

Deliverables:

- Evaluation of an online service
- Report content

5.19 Nineteenth Sprint (19th)

Timeline:

- Start - 09.02.2023
- End - 10.02.2023

Activity to complete:

- 4.7 (Documentation)

Deliverables:

- Master poster
- Completed master thesis

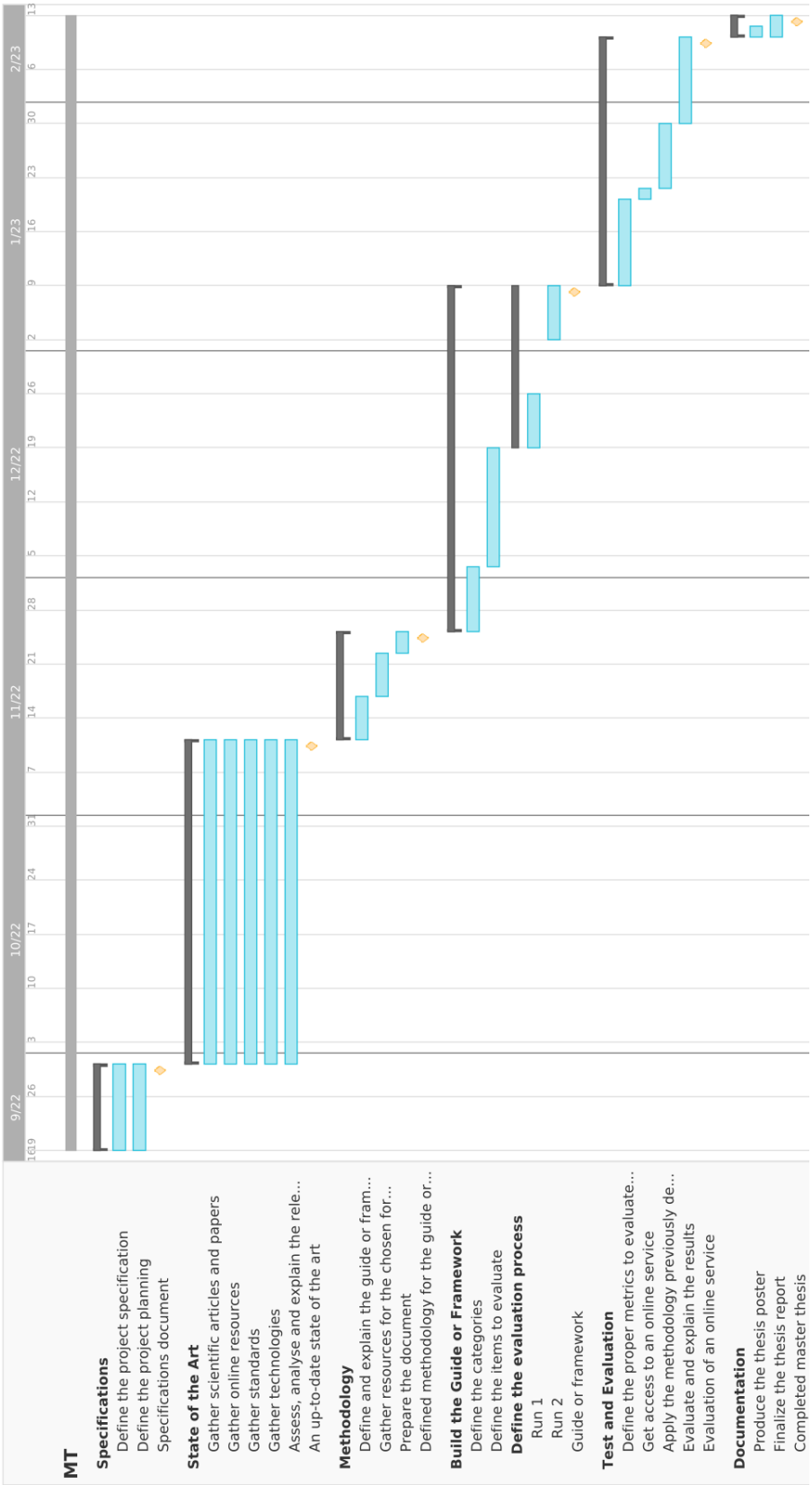

Figure 5.1 Gantt planning of the thesis

A | Appendices

A.1 Project Proposal

The next two pages are this thesis proposal form, submitted to the *University of Winchester*.

UNIVERSITY OF WINCHESTER

BS7205 – MSc Project

Project Proposal Form

Student Name: Loïc Guibert

Student Route:

Project Title: Provide Secured Environments for Artificial Intelligence Projects

Context:

In a world where Informational Technologies (*IT*) security is more and more proven and necessary, the need for new ways to secure and trust information systems is growing. This need is particularly expressed in the Artificial Intelligence (*AI*) field, where big amounts of data are periodically collected in order to improve services performances. Furthermore, such data is often personal and highly related to their user, which raise ethical and privacy-related questions.

Nowadays, end users of public or private online services are more and more aware of the personal data related risks and a change in consumption patterns is being noticed. New approaches must be developed in order to provide secured and privacy-first online services that can nevertheless enable a personalized experience.

Contribution:

By enabling secured and privacy-oriented personalized experience on online services, companies would be able to provide ethical, modern and respectful offers to their customers. All stakeholders would benefit from such an implementation, as long as the performance, time or processing capabilities do not restraint them in their activities.

This thesis aims to provide which technologies, best practices and safeguards can be integrated to information systems in order to ensure secured environments to the end users, particularly regarding *AI* projects. These components must then be implemented in a functional information system which includes *AI* processes, while providing a conclusion on the changes of such integration compared to the initial information system.

Literature Review:

Several emerging technologies that could fulfil the purpose of this thesis were found during preliminary research. Indeed, the academic world has new tools and increasingly permissive computing power, which opens up new possibilities.
Fully Homomorphic Encryption (*FHE*) shemes, that allows systems to process encrypted data without knowing its content, has make significant progress in terms of security, speed, and simplicity [Acar et al., 2017, 10.1145/3214303]. In terms of trustworthiness, a proposal of a new protocol, based on *HTTPS*, named HTTPA [King and Wang, 2021] aims to ensure to users of an online service that their related processes are executed in a trustable and attestable environment. This technology is not yet standardized nor reviewed. Regarding decentralized approaches, Federated Learning techniques could enable users to stay in control of their data by bringing the Machine Learning processes in their devices, which avoid data sharing to centralized systems. In latter researches, several models have been tested in various situations, where some aspects brought by this technique must be handled such as the heterogeneity of the data and the parties [Li et al., 2021, 10.1109/TKDE.2021.3124599]

Research Methodology and Research Design:

Seven steps have been defined in order to reach this thesis objectives. Each of them focuses on a particular subject and will be documented. The first steps will supply an academical view, and the last ones will use this knowledge to suggest a usable proposal.

- Provide an up-to-date literature review
- Analyse the current state-of-the-art
- List and compare related technologies, papers and resources

- Select the most appropriate items
- Build a guide or framework to explain how to evaluate an online service
- Test and validate the guide or framework

Change notification report

The following table is for you to report any changes to your project. After this proposal has been agreed, you should only change the table below – the content above should remain the same. For all changes, you must consult your academic supervisor

Date of Change	Brief Description of Change

Project Proposal Sign Off

I confirm:

a) I have discussed my proposed project with my allocated supervisor
b) I will not collect any data until my ethics application has received a favourable opinion from the appropriate university representatives
c) I will not collect any data without prior agreement from my academic supervisor
d) I will inform my academic supervisor of any changes to this proposal
e) This project is appropriate for my registered programme route

Student signature	
Print name	
Date	

I confirm:

a) This project is academically appropriate for a level 7 qualification
b) This project is appropriate for the route the student is registered to complete

Supervisor signature	
Print name	
Date	

References

[1] *Loïc Guibert / Master Thesis · GitLab*. Loïc Guibert, Sept. 2022. url: https://gitlab.forge.hefr.ch/loic.guibert/mt.

Glossary

AI Artificial Intelligence. 3, 5, 6

DL Deep Learning. 5

framework A framework is a set of software components used to bring new possibilities for the development of an IT tool, especially by providing elements related to its infrastructure. Outside of the IT field, it describes a set of rules, practices or must-haves in order to achieve a goal. 5–8, 12, 14

HEIA-fr School of Engineering and Architecture of Fribourg. 1

IT Informational Technologies. 3

ML Machine Learning. 5

Scrum Project management approach that aims to divide the work into sprints, with tasks defined by the team. 9