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	