ECS Project Information Form

Name: Thomas Green
Course: ENGR489
Supervisor: Arman Khouzani

Project Name:
Implementation of a Privacy-Preserving Machine Learning Model Using Homomorphic Encryption

Project Description:
This project explores the feasibility of implementing a privacy-preserving machine learning (ML) model using fully homomorphic encryption (FHE). As data security becomes increasingly critical across business sectors, solutions that enable computation on encrypted data, without revealing raw inputs, are gaining importance. This project proposes FHE as a solution to this, as a cryptographic method that allows operations to be performed directly on encrypted data, offering strong privacy guarantees. This project will use open-source libraries to train and evaluate basic ML models entirely on encrypted inputs, assessing performance, accuracy, and usability compared to an unencrypted baseline. While a working prototype and user interface may be developed to demonstrate real-world applications, the primary goal is to evaluate whether FHE is a viable and practical solution for secure ML under current technological constraints.

RISK ANALYSIS

Does your project contain anything that can cause serious harm or death?
e.g. building /modifying things with voltages over 60V, Chemicals, Moving machinery (e.g. Tank/Marvin) , Flying components (e.g. Phantom UAV, Plane), Bodies of water.

YES □ (Major) NO ☑

If Yes
Please contact the School Safety Officer or Electronics Technicians to talk through your Safety Plan

Otherwise

Does your project contain anything that can cause **harm or Injury?**
eg building /modifying things with voltages up to 60V, Moving machinery (e.g. desktop Minions), Flying components e.g. (micro Quad rotor, Parrot AR Drone, heavy items)

YES □ (Medium) NO ☑

If Yes, please Complete a Safety Plan, and send to Safety Officer

Everyone to complete.

Computers are an integral part of all projects. Describe how you will manage computer related risks such as Occupational Over Use, Cable management, etc.

I have identified four risks in total for my project and provided the appropriate controls and mitigations to them:

- The first risk category is human-factors, where the hazard is prolonged computer use. The risk is repetitive strain injury and eye strain, with the impact as medium, and the controls/mitigations are taking regular breaks (every 1 hour), maintain proper posture, adjust screen height and lighting.
- The second risk category is electrical, where the hazard is use of personal laptop and charging equipment. The risk is electrical faults and overheating, with the impact as low, and the controls/mitigations are ensuring cables are in good condition, avoid overloading outlets, use tested power sources.
- The third risk category is data security, where the hazard is loss of work or sensitive files. The risk is accidental data deletion or breach, with the impact as medium, and the control/mitigations are using version control (GitLab), back up code regularly, follow good data handling practices.
- The fourth risk is mental health, where the hazard is project stress or fatigue. The risk is reduced well-being and burnout, with the impact as medium, and the controls/mitigations are set manageable goals, communicate with supervisor, maintain healthy study habits.

General Project information – if in any doubt select yes.

Is your Project (it may be both.)

In-house e.g. internal school project ☑ Industry based or have an external client □

In your project will you being working or testing at any industry workplace or external sites. This includes meetings at client offices, or visits to sites.

YES □ NO ☑

Have you been Health and Safety inducted into the industry workplace or external sites

YES □ NO ☑

Does your Project use human test subjects?

YES □ NO ☑

Will you have Ethics Approval before you start testing?

YES □ NO ☑

If you have any doubts on which category your project falls into please contact the School Safety Officer, to help evaluate the safe risk.