ML Model Sharing Survey

This survey is part of an academic research project conducted by researchers from NECSTLab (Politecnico di Milano). All responses are anonymous and will be used strictly for research purposes.

If you have any questions or need further information, feel free to contact the research team at:
gabriele.digregorio@polimi.it
marco.digennaro@polimi.it

* Indicates required question

1. Which of the following best describes your area of expertise? *

Mark only one oval.

- ◯ Machine Learning / Artificial Intelligence
- ◯ Cybersecurity
- ◯ Software Engineering
- ◯ Data Science
- ◯ Robotics / Control Systems / Automation
- ◯ Bioinformatics
- ◯ Other: _____

2. How would you rate your level of expertise in the field of Machine Learning? *

Mark only one oval.

	1	2	3	4	5	
Basi	◯	◯	◯	◯	◯	Expert

3. Have you ever loaded a pre-trained machine learning model onto your system or computer that was shared by someone else or downloaded from the internet? *

Mark only one oval.

- ◯ Yes
- ◯ No

Consider a pre-trained ML model that someone has shared with you or that you have downloaded from the internet. Please answer the following questions.

If needed, feel free to consult the official documentation:
- Keras documentation
- PyTorch documentation

4. Given this snippet of code, how comfortable would you feel when loading the shared model? *

```
import keras

model = keras.models.load_model("model.keras", safe_mode=False)
```

Mark only one oval.

	1	2	3	4	5	6	7	8	9	10	
Not at all comfortable	◯	◯	◯	◯	◯	◯	◯	◯	◯	◯	Totally comfortable – I would trust and use the model

5. If you feel that the previous situation raises any concerns, which one(s)?

Check all that apply.

- ☐ Poor performance
- ☐ Manipulated training process
- ☐ Arbitrary code execution
- ☐ Licensing
- ☐ Challenging to ensure ethical AI compliance
- ☐ Other: _____

6. Given this snippet of code, how comfortable would you feel when loading the shared model? *

```
import keras

model = keras.models.load_model("model.keras", safe_mode=True)
```

Mark only one oval.

	1	2	3	4	5	6	7	8	9	10	
Not at all comfortable	◯	◯	◯	◯	◯	◯	◯	◯	◯	◯	Totally comfortable – I would trust and use the model

7. If you feel that the previous situation raises any concerns, which one(s)?

Check all that apply.

- [ ] Poor performance
- [ ] Manipulated training process
- [ ] Arbitrary code execution
- [ ] Licensing
- [ ] Challenging to ensure ethical AI compliance
- [ ] Other: _____

8. Given this snippet of code, how comfortable would you feel when loading the shared model? *

```
import torch

torch.load("model.pt", weights_only=False)
```

Mark only one oval.

	1	2	3	4	5	6	7	8	9	10	
Not at all comfortable	◯	◯	◯	◯	◯	◯	◯	◯	◯	◯	Totally comfortable – I would trust and use the model

9. If you feel that the previous situation raises any concerns, which one(s)?

Check all that apply.

- [ ] Poor performance
- [ ] Manipulated training process
- [ ] Arbitrary code execution
- [ ] Licensing
- [ ] Challenging to ensure ethical AI compliance
- [ ] Other: _____

10. Given this snippet of code, how comfortable would you feel when loading the shared model? *

Note: This question also includes the process of importing the model definition or code provided by the same source from which you downloaded the model weights.

```
import torch

'''
[OMITTED]
Import of the model class from an external file
dowloaded together with model_weights.pt
'''

torch.load("model_weights.pt", weights_only=True)
```

Mark only one oval.

	1	2	3	4	5	6	7	8	9	10	
Not	◯	◯	◯	◯	◯	◯	◯	◯	◯	◯	Totally comfortable – I would trust and use the model almost as before

11. If you feel that the previous situation raises any concerns, which one(s)?

Check all that apply.

- [ ] Poor performance
- [ ] Manipulated training process
- [ ] Arbitrary code execution
- [ ] Licensing
- [ ] Challenging to ensure ethical AI compliance
- [ ] Other: _____

12. Have you ever inspected a shared model file before loading it? *

This means performing actions such as unzipping the file (if required by the format), understanding the files it contains, reviewing their contents, and evaluating the internals of the model before loading it into your system.

Mark only one oval.

- ◯ Yes
- ◯ No

13. Knowing that platforms like Hugging Face provide security tools for their repositories, including malware scanning, pickle scanning, secrets scanning, and third-party AI model scanners such as JFrog and Protect AI—if the shared model you were to load was downloaded from such platforms, would your perception of comfort in doing so change? *

Mark only one oval.

- ◯ I would feel less comfortable loading the model
- ◯ It would not affect my perception
- ◯ I would feel more comfortable loading the model

14. If you feel that the previous situation raises any concerns, which one(s)?

Check all that apply.

- [ ] Poor performance
- [ ] Manipulated training process
- [ ] Arbitrary code execution
- [ ] Licensing
- [ ] Challenging to ensure ethical AI compliance
- [ ] Other: _____