

CLAIMS

1. A computer-implemented method for private transfer learning, comprising:
 - providing authorized use of a machine learning model that is trained to perform a generic task by a deep neural network (DNN), by:
 - encrypting the machine learning model using a predetermined encryption mechanism, wherein the machine learning model comprises a training application programming interface (API), an inferencing API, and credentials that:
 - are programmed into the machine learning model;
 - define who can train the machine learning model;
 - define how the machine learning model can be trained; and
 - authenticate a call from an unsecured execution environment;
 - copying the encrypted machine learning model to a trusted execution environment; and
 - performing private transfer learning by training the machine learning model to perform a task that is more specific than the generic task by executing the training API in a secure enclave of the trusted execution environment, wherein training the machine learning model comprises authenticating, using the credentials, a call to execute the training API from the unsecured execution environment.
2. The method of claim 1, further comprising generating an inference from the machine learning model by executing the inferencing API in the secure enclave of the trusted execution environment.
3. The method of claim 1, further comprising generating a combination of a body of the machine learning model with a head of an additional machine learning model in the trusted execution environment.
4. The method of claim 3, further comprising performing the inferencing API for the combination.
5. The method of claim 3, further comprising performing the training API for the combination.
6. A computer program product comprising program instructions stored on a computer readable storage medium, wherein the computer readable storage medium is not a transitory signal per se, the program instructions executable by a processor to cause the processor to perform a method comprising:
 - providing authorized use of a machine learning model that is trained to perform a generic task by a deep neural network (DNN), by:
 - encrypting the machine learning model using a predetermined encryption mechanism, wherein the machine learning model comprises a training application programming interface (API), an inferencing API, and credentials that:
 - are programmed into the machine learning model;

define who can train the machine learning model;
 define how the machine learning model can be trained; and
 authenticate a call from an unsecured execution environment;
 copying the encrypted machine learning model to a trusted execution environment; and
 performing private transfer learning by training the machine learning model to perform a task that
 is more specific than the generic task by executing the training API in a secure enclave of the trusted
 execution environment, wherein training the machine learning model comprises authenticating, using the
 credentials, a call to execute the training API from the unsecured execution environment.

7. The computer program product of claim 6, the method further comprising generating an inference from the machine learning model by executing the inferencing API in the secure enclave of the trusted execution environment.

8. The computer program product of claim 6, the method further comprising generating a combination of a body of the machine learning model with a head of an additional machine learning model in the trusted execution environment.

9. The computer program product of claim 8, the method further comprising performing the inferencing API for the combination.

10. The computer program product of claim 8, the method further comprising performing the training API for the combination.

11. A system comprising:

a computer processing circuit; and

a computer-readable storage medium storing instructions, which, when executed by the computer processing circuit, are configured to cause the computer processing circuit to perform a method comprising:

providing authorized use of a machine learning model that is trained to perform a generic task by a deep neural network (DNN), by:

encrypting the machine learning model using a predetermined encryption mechanism, wherein the machine learning model comprises a training application programming interface (API), an inferencing API, and credentials that:

are programmed into the machine learning model;

define who can train the machine learning model;

define how the machine learning model can be trained; and

authenticate a call from an unsecured execution environment;

copying the encrypted machine learning model to a trusted execution environment; and
 performing private transfer learning by training the machine learning model to perform a task that is more specific than the generic task by executing the training API in a secure enclave of the trusted execution environment, wherein training the machine learning model comprises authenticating, using the credentials, a call to execute the training API from the unsecured execution environment.

12. The system of claim 11, the method further comprising generating an inference from the machine learning model by executing the inferencing API in the secure enclave of the trusted execution environment.

13. The system of claim 11, the method further comprising generating a combination of a body of the machine learning model with a head of an additional machine learning model in the trusted execution environment.

14. The system of claim 13, the method further comprising performing the inferencing API for the combination.

15. The system of claim 13, the method further comprising performing the training API for the combination.

16. A system comprising:

a computer processing circuit;

a graphical processing circuit (GPU); and

a computer-readable storage medium storing instructions, which, when executed by the computer processing circuit, are configured to cause the computer processing circuit to perform a method comprising:

providing authorized use of a machine learning model that is trained to perform a generic task by a deep neural network (DNN), by:

encrypting the machine learning model using a predetermined encryption mechanism, wherein the machine learning model comprises a training application programming interface (API), an inferencing API, and credentials that:

are programmed into the machine learning model;

define who can train the machine learning model;

define how the machine learning model can be trained; and

authenticate a call from an unsecured execution environment;

copying the encrypted machine learning model to a trusted execution environment; and

performing private transfer learning by training the machine learning model to perform a task that is more specific than the generic task by executing the training API in a secure enclave of the trusted execution environment, wherein training the machine learning model comprises authenticating, based on the credentials, a call to execute the training API from the unsecured execution environment.

17. A computer-implemented method for private transfer learning, comprising:
providing authorized use of a machine learning model that is trained to perform a generic task by a deep neural network (DNN), by:

 encrypting the machine learning model using a predetermined encryption mechanism, wherein the machine learning model comprises a training application programming interface (API), an inferencing API, and credentials that:

 are programmed into the machine learning model;
 define who can train the machine learning model;
 define how the machine learning model can be trained; and
 authenticate a call from an unsecured execution environment;

 copying the encrypted machine learning model to a trusted execution environment; and

 performing private transfer learning by training the machine learning model to perform a task that is more specific than the generic task by executing the training API in a secure enclave of the trusted execution environment, wherein training the machine learning model comprises authenticating, based on the credentials, a call to execute the training API from the unsecured execution environment.

18. The method of claim 17, wherein:

 the machine learning model comprises a deep neural network (DNN) model;

 the DNN model is trained to perform a generic task; and

 the training API trains the DNN model to perform a task that refines the generic task to a more specific task than the generic task.