

WHAT IS CLAIMED IS:

1 1. A method comprising:
2 receiving, by a secure platform computer operating a secure
3 memory space, a first portion and a second portion of project data corresponding
4 to a federated project involving a first entity and a second entity, the first portion
5 of the project data corresponding to the first entity and the second portion of the
6 project data corresponding to the second entity;
7 receiving, by the secure platform computer, a first data set of the
8 first entity and a second data set of the second entity;
9 generating, by the secure platform computer, a machine-learning
10 model based at least in part on the first data set, the second data set, and the
11 project data; and
12 providing, by the secure platform computer, access to the machine-
13 learning model to the first entity and the second entity, the machine-learning
14 model being stored within the secure memory space.

1 2. The method of claim 1, wherein the first data set and the
2 second data set are encrypted and wherein the method further comprises
3 decrypting, by the secure platform computer, the first data set and the second
4 data set prior to generating the machine-learning model.

1 3. The method of claim 1, further comprising:
2 receiving, by the secure platform computer, a first public key for the
3 first entity; and
4 verifying, by the secure platform computer, integrity of the first data
5 set based at least in part on verifying one or more digital signatures
6 corresponding to one or more received messages comprising the first data set,
7 the one or more digital signatures being verified utilizing the first public key.

1 4. The method of claim 1, further comprising:
2 receiving, by the secure platform computer via an application
3 programming interface (API), input data from a computing device associated with
4 the first entity;

5 providing, by the secure platform computer, the input data to the
6 machine-learning model as input;
7 receiving, by the secure platform computer, output data from the
8 machine-learning model; and
9 providing, by the secure platform computer via the API, the output
10 data to the computing device associated with the first entity.

1 5. The method of claim 4, further comprising:
2 modifying, by the secure platform computer, the first data set to
3 include the input data; and
4 updating, by the secure platform computer, the machine-learning
5 model based at least in part on the first data set as modified.

1 6. The method of claim 1, wherein the project data comprises a
2 first schema associated with the first data set, the first schema defining a data
3 structure for data of the first data set, and wherein the method further comprises
4 validating, by the secure platform computer, the first data set based at least in
5 part on the first schema.

1 7. The method of claim 1, wherein the project data comprises
2 permissive use information, and wherein the method further comprises:
3 generating, by the secure platform computer, a usage policy
4 associated with the machine-learning model based at least in part on the
5 permissive use information; and
6 verifying, by the secure platform computer, that subsequent use of
7 the machine-learning model is in conformance with the usage policy.

1 8. The method of claim 1, further comprising:
2 providing, by the secure platform computer, an interface for
3 verifying security of the secure memory space and integrity of the first data set
4 and the second data set.

1 9. A computing device, comprising:
2 one or more processors;
3 a secure platform computer operating a secure memory space, the
4 secure memory space comprising computer-executable instructions that, when

5 executed by the one or more processors, causes the secure platform computer
6 to:

7 receive a first portion and a second portion of project data
8 corresponding to a federated project involving a first entity and a second
9 entity, the first portion of the project data corresponding to the first entity
10 and the second portion of the project data corresponding to the second
11 entity;

12 receive a first data set of the first entity and a second data
13 set of the second entity;

14 generate a machine-learning model based at least in part on
15 the first data set, the second data set, and the project data;

16 provide access to the machine-learning model to the first
17 entity and the second entity, the machine-learning model being stored
18 within the secure memory space.

1 10. The computing device of claim 9, wherein the secure
2 memory space is an enclave managed by a chip set of the one or more
3 processors, wherein the enclave is encrypted by the chip set and accessible only
4 by the chip set.

1 11. The computing device of claim 9, wherein the instructions
2 further cause the secure platform computer to maintain an immutable ledger
3 comprising information corresponding to receipt of the first data set and the
4 second data set by the secure platform computer.

1 12. The computing device of claim 11, wherein the instructions
2 further cause the secure platform computer to:

3 receive, from a requesting entity, a task request requesting the
4 immutable ledger be verified;

5 compare a first identifier of the requesting entity to a second
6 identifier of the project data;

7 when the first identifier matches the second identifier, verifying the
8 immutable ledger; and

9 providing, to the requesting entity, an indication that the immutable
10 ledger was verified.

1 13. The computing device of claim 12, wherein the immutable
2 ledger further comprises an identifier for a provider of the data, and where the
3 instructions further cause the secure platform computer to verify, that the provider
4 of the data corresponds to the first entity or the second entity.

1 14. The computing device of claim 12, wherein the instructions
2 further cause the secure platform computer to generate one or more first keys for
3 retrieving the first data set from the secure memory space and one or more
4 second keys for retrieving the second data set from the secure memory space.

1 15. The computing device of claim 14, wherein information
2 maintained in the immutable ledger comprises first hash values corresponding to
3 the one or more first keys and second hash values corresponding to the one or
4 more second keys.

1 16. The computing device of claim 9, wherein the instructions
2 further cause the secure platform computer to:
3 generate an additional machine-learning model based at least in
4 part on the first data set, the second data set, and the project data; and
5 provide access to the additional machine-learning model for the first
6 entity, the additional machine-learning model being stored within the secure
7 memory space.

1 17. The computing device of claim 9, wherein the instructions
2 further cause the secure platform computer to:
3 transmit a notification to the second entity in response to receiving
4 the first portion of the project data, the notification being transmitted prior to
5 receiving the second portion of the project data, wherein the notification indicates
6 receipt of the first portion of the project data.

1
1 18. The computing device of claim 9, wherein the first data set is
2 inaccessible by the second entity and wherein the second data set is inaccessible
3 by the first entity.

1 19. The computing device of claim 9, wherein the instructions
2 further cause the secure platform computer to transmit a notification to the first
3 entity and the second entity, wherein the notification indicates generation of the
4 machine-learning model is complete.

1 20. The computing device of claim 9, wherein the instructions
2 further cause the secure platform computer to:
3 receive, from a computing device of the first entity, a task request
4 indicative of a request to update the machine-learning model;
5 update the machine-learning model utilizing a data set comprising
6 the first data set, the second data set, and subsequent data received after receipt
7 of the first data set and the second data set; and
8 transmit, to the computing device of the first entity, a notification
9 indicating the task request was successful or unsuccessful.