

WHAT IS CLAIMED IS:

1. A method, comprising:
generating, with at least one processor, a data repository;
receiving, with the at least one processor, a private set intersection (PSI) data query, wherein the PSI data query comprises a match parameter for performing the PSI data query on the data repository;
transmitting, with the at least one processor, a data classification encryption key for encrypting a data field of a transaction data record associated with an entity, wherein the data classification encryption key is associated with a data field that corresponds to a match parameter data field of the match parameter;
determining, with the at least one processor, whether to authorize the PSI data query on the data repository;
transmitting, with the at least one processor, a data authorization encryption key based on determining to authorize the PSI data query on the data repository, wherein the data authorization encryption key is for encrypting an encrypted data field of a transaction data record associated with an entity to provide a two-layer encrypted data field; and
performing, with the at least one processor, the PSI data query on the data repository.

2. The method of claim 1, further comprising:
generating a PSI result based on performing the PSI data query on the data repository;
providing the PSI result as an input to a machine learning algorithm; and
generating an output of the machine learning algorithm based on the input.

3. The method of claim 1, wherein generating the data repository comprises:
encrypting a first data field of a first transaction data record associated with a first entity with a first data classification encryption key to provide an encrypted first data field of the first transaction data record associated with the first entity, wherein the first data classification encryption key is assigned according to a classification of the first data field of the first transaction data record and the first entity;

encrypting a second data field of the first transaction data record associated with the first entity with a second data classification encryption key to provide an encrypted second data field of the first transaction data record associated with the first entity, wherein the second data classification encryption key is assigned according to a classification of the second data field of the first transaction data record and the first entity;

encrypting a first data field of a second transaction data record associated with a second entity with a third data classification encryption key to provide an encrypted first data field of the second transaction data record associated with the second entity, wherein the third data classification encryption key is assigned according to a classification of the first data field of the second transaction data record and the second entity; and

encrypting a second data field of the second transaction data record associated with the second entity with a fourth data classification encryption key to provide an encrypted second data field of the second transaction data record associated with the second entity, wherein the fourth data classification encryption key is assigned according to a classification of the second data field of the second transaction data record and the second entity.

4. The method of claim 3, wherein generating the data repository comprises:

encrypting the encrypted first data field of the first transaction data record associated with the first entity with a first data authorization encryption key to provide a two-layer encrypted first data field of the first transaction data record associated with the first entity, wherein the first data authorization encryption key is assigned according to the first entity;

encrypting the encrypted first data field of the second transaction data record associated with the second entity with a second data authorization encryption key to provide a two-layer encrypted first data field of the second transaction data record associated with the second entity, wherein the second data authorization encryption key is assigned according to the second entity;

storing the two-layer encrypted first data field of the first transaction data record associated with the first entity in the data repository; and

storing two-layer encrypted first data field of the second transaction data record associated with the second entity in the data repository.

5. The method of claim 3, wherein generating the data repository comprises:

storing the encrypted second data field of the first transaction data record associated with the first entity in the data repository; and

storing the encrypted second data field of the second transaction data record associated with the second entity in the data repository.

6. The method of claim 1, wherein the PSI data query further comprises an authorization parameter associated with the match parameter, wherein determining whether to authorize the PSI data query on the data repository comprises:

transmitting a request for authorization based on the PSI data query;

receiving a response for authorization, wherein the response for authorization comprises transaction data associated with the match parameter;

determining that the transaction data associated with the match parameter included in the response for authorization corresponds to the authorization parameter associated with the match parameter; and

determining to authorize the PSI data query based on determining that the transaction data associated with the match parameter corresponds to the authorization parameter associated with the match parameter.

7. The method of claim 1, wherein receiving the PSI data query comprises: receiving the PSI data query from a submission entity; and

wherein transmitting the data authorization encryption key comprises:

transmitting the data authorization encryption key to the submission entity based on determining to authorize the PSI data query on the data repository.

8. A system, comprising:

a data repository hosting system comprising at least one processor programmed or configured to:

generate a data repository;

receive, from a submission entity system associated with a submission entity, a private set intersection (PSI) data query, wherein the PSI data query

comprises a match parameter for performing the PSI data query on the data repository;

transmit, to the submission entity system, a data classification encryption key for encrypting a data field of a transaction data record associated with an entity, wherein the data classification encryption key is associated with a data field that corresponds to a match parameter data field of the match parameter;

determine whether to authorize the PSI data query on the data repository;

transmit, to the submission entity system, a data authorization encryption key based on determining to authorize the PSI data query on the data repository, wherein the data authorization encryption key is for encrypting an encrypted data field of a transaction data record associated with an entity to provide a two-layer encrypted data field; and

perform the PSI data query on the data repository.

9. The system of claim 8, wherein the at least one processor is further programmed or configured to:

generate a PSI result based on performing the PSI data query on the data repository; and

transmit the PSI result to the submission entity system,

wherein the submission entity system is programmed or configured to:

provide the PSI result as an input to a machine learning algorithm; and

generate an output of the machine learning algorithm based on the input.

10. The system of claim 8, wherein, when generating the data repository, the at least one processor is programmed or configured to:

encrypt a first data field of a first transaction data record associated with a first entity with a first data classification encryption key to provide an encrypted first data field of the first transaction data record associated with the first entity, wherein the first data classification encryption key is assigned according to a classification of the first data field of the first transaction data record and the first entity;

encrypt a second data field of the first transaction data record associated with the first entity with a second data classification encryption key to provide an encrypted second data field of the first transaction data record associated with the first entity, wherein the second data classification encryption key is assigned according to a classification of the second data field of the first transaction data record and the first entity;

encrypt a first data field of a second transaction data record associated with a second entity with a third data classification encryption key to provide an encrypted first data field of the second transaction data record associated with the second entity, wherein the third data classification encryption key is assigned according to a classification of the first data field of the second transaction data record and the second entity; and

encrypt a second data field of the second transaction data record associated with the second entity with a fourth data classification encryption key to provide an encrypted second data field of the second transaction data record associated with the second entity, wherein the fourth data classification encryption key is assigned according to a classification of the second data field of the second transaction data record and the second entity.

11. The system of claim 10, wherein, when generating the data repository, the at least one processor is programmed or configured to:

encrypt the encrypted first data field of the first transaction data record associated with the first entity with a first data authorization encryption key to provide a two-layer encrypted first data field of the first transaction data record associated with the first entity, wherein the first data authorization encryption key is assigned according to the first entity;

encrypt the encrypted first data field of the second transaction data record associated with the second entity with a second data authorization encryption key to provide a two-layer encrypted first data field of the second transaction data record associated with the second entity, wherein the second data authorization encryption key is assigned according to the second entity;

store the two-layer encrypted first data field of the first transaction data record associated with the first entity in the data repository; and

store two-layer encrypted first data field of the second transaction data record associated with the second entity in the data repository.

12. The system of claim 10, wherein, when generating the data repository, the at least one processor is programmed or configured to:

store the encrypted second data field of the first transaction data record associated with the first entity in the data repository; and

store the encrypted second data field of the second transaction data record associated with the second entity in the data repository.

13. The system of claim 8, wherein the PSI data query further comprises an authorization parameter associated with the match parameter, wherein, when determining whether to authorize the PSI data query on the data repository, the at least one processor is programmed or configured to:

transmit a request for authorization based on the PSI data query;

receive a response for authorization, wherein the response for authorization comprises transaction data associated with the match parameter;

determine that the transaction data associated with the match parameter included in the response for authorization corresponds to the authorization parameter associated with the match parameter; and

determine to authorize the PSI data query based on determining that the transaction data associated with the match parameter corresponds to the authorization parameter associated with the match parameter.

14. The system of claim 8, wherein, when transmitting the data authorization encryption key, the at least one processor is programmed or configured to:

transmit the data authorization encryption key to the submission entity system based on determining to authorize the PSI data query on the data repository.

15. A computer program product comprising at least one non-transitory computer-readable medium including one or more instructions that, when executed by at least one processor, cause the at least one processor to:

generate a data repository;

receive a private set intersection (PSI) data query, wherein the PSI data query comprises a match parameter for performing the PSI data query on the data repository;

transmit a data classification encryption key for encrypting a data field of a transaction data record associated with an entity, wherein the data classification encryption key is associated with a data field that corresponds to a match parameter data field of the match parameter;

determine whether to authorize the PSI data query on the data repository;

transmit a data authorization encryption key based on determining to authorize the PSI data query on the data repository, wherein the data authorization encryption key is for encrypting an encrypted data field of a transaction data record associated with an entity to provide a two-layer encrypted data field; and

perform the PSI data query on the data repository.

16. The computer program product of claim 15, wherein the one or more instructions, when executed by at least one processor, further cause the at least one processor to:

generate a PSI result based on performing the PSI data query on the data repository;

provide the PSI result as an input to a machine learning algorithm; and

generate an output of the machine learning algorithm based on the input.

17. The computer program product of claim 15, wherein, the one or more instructions that cause the at least one processor to generate the data repository, cause the at least one processor to:

encrypt a first data field of a first transaction data record associated with a first entity with a first data classification encryption key to provide an encrypted first data field of the first transaction data record associated with the first entity, wherein the first data classification encryption key is assigned according to a classification of the first data field of the first transaction data record and the first entity;

encrypt a second data field of the first transaction data record associated with the first entity with a second data classification encryption key to provide an encrypted second data field of the first transaction data record associated with the first entity, wherein the second data classification encryption key is assigned according to a classification of the second data field of the first transaction data record and the first entity;

encrypt a first data field of a second transaction data record associated with a second entity with a third data classification encryption key to provide an encrypted first data field of the second transaction data record associated with the second entity, wherein the third data classification encryption key is assigned according to a classification of the first data field of the second transaction data record and the second entity; and

encrypt a second data field of the second transaction data record associated with the second entity with a fourth data classification encryption key to provide an encrypted second data field of the second transaction data record associated with the second entity, wherein the fourth data classification encryption key is assigned according to a classification of the second data field of the second transaction data record and the second entity.

18. The computer program product of claim 17, wherein, the one or more instructions that cause the at least one processor to generate the data repository, cause the at least one processor to:

encrypt the encrypted first data field of the first transaction data record associated with the first entity with a first data authorization encryption key to provide a two-layer encrypted first data field of the first transaction data record associated with the first entity, wherein the first data authorization encryption key is assigned according to the first entity;

encrypt the encrypted first data field of the second transaction data record associated with the second entity with a second data authorization encryption key to provide a two-layer encrypted first data field of the second transaction data record associated with the second entity, wherein the second data authorization encryption key is assigned according to the second entity;

store the two-layer encrypted first data field of the first transaction data record associated with the first entity in the data repository; and

store two-layer encrypted first data field of the second transaction data record associated with the second entity in the data repository.

19. The computer program product of claim 17, wherein, the one or more instructions that cause the at least one processor to generate the data repository, cause the at least one processor to:

store the encrypted second data field of the first transaction data record associated with the first entity in the data repository; and

store the encrypted second data field of the second transaction data record associated with the second entity in the data repository.

20. The computer program product of claim 15, wherein the PSI data query further comprises an authorization parameter associated with the match parameter, wherein, the one or more instructions that cause the at least one processor to determine whether to authorize the PSI data query on the data repository, cause the at least one processor to:

transmit a request for authorization based on the PSI data query;

receive a response for authorization, wherein the response for authorization comprises transaction data associated with the match parameter;

determine that the transaction data associated with the match parameter included in the response for authorization corresponds to the authorization parameter associated with the match parameter; and

determine to authorize the PSI data query based on determining that the transaction data associated with the match parameter corresponds to the authorization parameter associated with the match parameter.