CLAIMS

1. A method for performing secure computing while maintaining data confidentiality, the method comprising:

receiving, via an application on a computing device, both data and a request to perform a secure operation on the data, wherein the secure operation is to be performed using a secure compute engine on a cloud platform such that the data is not viewable to a provider of the cloud platform;

in response to determining that the secure operation to be performed using the secure compute engine matches an operation in a history of past requests associated with an authorized user, applying transformations to the data so that the data is not viewable to the provider by:

constructing a chain of pre-processing operations that (1) converts incompatible attributes of the data with the secure compute engine into compatible attributes and (2) protects information in the data using a cryptographic technique on the data with compatible attributes; and

executing the chain of pre-processing operations using an engine connector that facilitates communication between the secure compute engine and an application programming interface (API) of the application, wherein the execution generates transformed data;

transmitting the transformed data to the secure compute engine on the cloud platform to perform the secure operation on the transformed data;

receiving a result of the secure operation from the secure compute engine; and

transmitting the result to the application.

2. The method of claim 1, wherein transmitting the result to the application further comprises:

constructing a chain of post-processing operations that reverses the transformations to generate a finalized result, wherein the finalized result equals a potential result acquired if the secure operation was directly performed on the data without the transformations; and

executing the chain of post-processing operations via the application.

3. The method of claim 1, wherein the secure compute engine is further configured to:

receive additional transformed data from another application on at least one other computing device;

combine the transformed data with the additional transformed data to create aggregated transformed data;

perform the secure operation on the aggregated transformed data; and

transmit a combined result to the application of the computing device and the another application on the at least one other computing device.

4. The method of claim 1, wherein a user of the computing device specifies, over a user interface of the application, operations from a store of operations to include in the chain of pre-processing operations.

5. The method of claim 1, further comprising validating the request based on a user identifier of the authorized user.

6. The method of claim 1, wherein the cryptographic technique is at least one of Shamir's secret sharing and homomorphic encryption.

7. The method of claim 1, wherein the chain of pre-processing operations comprises at least one of removing, anonymizing, tokenizing, replacing, and truncating data fields of the data.

8. The method of claim 1, wherein the secure operation comprises determining at least one of (1) descriptive statistics comprising average, standard deviation, and median, (2) predictive statistics comprising linear regression, logistic regression, and classification, and (3) custom functions comprising credit scoring.

9. A system for performing secure computing while maintaining data confidentiality, the system comprising:

a hardware processor configured to:

receive, via an application on a computing device, both data and a request to perform a secure operation on the data, wherein the secure operation is to be performed using a secure compute engine on a cloud platform such that the data is not viewable to a provider of the cloud platform;

in response to determining that the secure operation to be performed using the secure compute engine matches an operation in a history of past requests associated with an authorized user, apply transformations to the data so that the data is not viewable to the provider by:

constructing a chain of pre-processing operations that (1) converts incompatible attributes of the data with the secure compute engine into compatible attributes and (2) protects information in the data using a cryptographic technique on the data with compatible attributes; and

executing the chain of pre-processing operations using an engine connector that facilitates communication between the secure compute engine and an application programming interface (API) of the application, wherein the execution generates transformed data;

transmit the transformed data to the secure compute engine on the cloud platform to perform the secure operation on the transformed data;

receive a result of the secure operation from the secure compute engine; and

transmit the result to the application.

10. The system of claim 9, wherein the hardware processor is configured to transmit the result to the application by:

constructing a chain of post-processing operations that reverses the transformations to generate a finalized result, wherein the finalized result equals a potential result acquired if the secure operation was directly performed on the data without the transformations; and

executing the chain of post-processing operations via the application.

11. The system of claim 9, wherein the secure compute engine is further configured to:

receive additional transformed data from another application on at least one other computing device;

combine the transformed data with the additional transformed data to create aggregated transformed data;

perform the secure operation on the aggregated transformed data; and

transmit a combined result to the application of the computing device and the another application on the at least one other computing device.

12. The system of claim 9, wherein a user of the computing device specifies, over a user interface of the application, operations from a store of operations to include in the chain of pre-processing operations.

13. The system of claim 9, wherein the hardware processor is further configured to validate the request based on a user identifier of the authorized user.

14. The system of claim 9, wherein the cryptographic technique is at least one of Shamir's secret sharing and homomorphic encryption.

15. The system of claim 9, wherein the chain of pre-processing operations comprises at least one of removing, anonymizing, tokenizing, replacing, and truncating data fields of the data.

16. The system of claim 9, wherein the secure operation comprises determining at least one of (1) descriptive statistics comprising average, standard deviation, and median, (2) predictive statistics comprising linear regression, logistic regression, and classification, and (3) custom functions comprising credit scoring.

17. A non-transitory computer readable medium storing thereon computer executable instructions for performing secure computing while maintaining data confidentiality, including instructions for:

receiving, via an application on a computing device, both data and a request to perform a secure operation on the data, wherein the secure operation is to be performed using a secure compute engine on a cloud platform such that the data is not viewable to a provider of the cloud platform;

in response to determining that the secure operation to be performed using the secure compute engine matches an operation in a history of past requests associated with an authorized user, applying transformations to the data so that the data is not viewable to the provider by:

constructing a chain of pre-processing operations that (1) converts incompatible attributes of the data with the secure compute engine into compatible attributes and (2) protects information in the data using a cryptographic technique on the data with compatible attributes; and

executing the chain of pre-processing operations using an engine connector that facilitates communication between the secure compute engine and an application programming interface (API) of the application, wherein the execution generates transformed data;

transmitting the transformed data to the secure compute engine on the cloud platform to perform the secure operation on the transformed data;

receiving a result of the secure operation from the secure compute engine; and

transmitting the result to the application.

18. The non-transitory computer readable medium of claim 17, wherein the instruction for transmitting the result to the application further comprises instructions for:

constructing a chain of post-processing operations that reverses the transformations to generate a finalized result, wherein the finalized result equals a potential result acquired if the secure operation was directly performed on the data without the transformations; and

executing the chain of post-processing operations via the application.

19. The non-transitory computer readable medium of claim 17, wherein the secure compute engine is further configured to:

receive additional transformed data from another application on at least one other computing device;

combine the transformed data with the additional transformed data to create aggregated transformed data;

perform the secure operation on the aggregated transformed data; and

transmit a combined result to the application of the computing device and the another application on the at least one other computing device.

20. The non-transitory computer readable medium of claim 17, wherein a user of the computing device specifies, over a user interface of the application, operations from a store of operations to include in the chain of pre-processing operations.