

**A LOGISTIC REGRESSION MODELING SCHEME USING SECRETE
SHARING
BACKGROUND**

[0001] Machine learning is a subset of data science that uses statistical models to draw insights and make predictions. To facilitate data exchange and cooperation, different parties may work together to establish a machine learning model. Traditional machine learning projects aggregate training data obtained from multiple parties in one place. Then, in the training phase of the machine learning process, a training model is built using machine learning tools based on the aggregated data, so that the model can be uniformly trained. The training data may be aggregated by any participating party, or at a third party that is trusted and selected by all participating parties.

SUMMARY

[0002] This specification describes training a multi-party secure logistic regression model (SLRM) by using secrete sharing (secret sharing) techniques.

[0003] In general, one innovative aspect of the subject matter described in this specification can be embodied in methods that include the actions of dividing sample training data for a secure logistic regression model (SLRM) into a plurality of shares using secret sharing (SS), wherein each share is distributed to a secure computation node (SCN); iteratively updating parameters associated with the SLRM using each share of the sample training data, wherein the iterative updating continues until the occurrence of a predetermined condition; and after iteratively updating the parameters associated with the SLRM, outputting a training result configured for use by each SCN. Other embodiments of this aspect include corresponding computer systems, apparatus, and computer programs recorded on one or more computer storage devices, each configured to perform the actions of the methods.

[0004] The foregoing and other embodiments can each optionally include one or more of the following features, alone or in combination. In particular, one embodiment includes all the following features in combination.

[0005] This specification also provides one or more non-transitory computer-readable storage media coupled to one or more processors and having instructions stored thereon which,

when executed by the one or more processors, cause the one or more processors to perform operations in accordance with implementations of the methods provided herein.

[0006] This specification further provides a system for implementing the methods provided herein. The system includes one or more processors, and a computer-readable storage medium coupled to the one or more processors having instructions stored thereon which, when executed by the one or more processors, cause the one or more processors to perform operations in accordance with implementations of the methods provided herein.

[0007] It is appreciated that methods in accordance with this specification may include any combination of the aspects and features described herein. That is, methods in accordance with this specification are not limited to the combinations of aspects and features specifically described herein, but also include any combination of the aspects and features provided.

[0008] The details of one or more implementations of this specification are set forth in the accompanying drawings and the description below. Other features and advantages of this specification will be apparent from the description and drawings, and from the claims.

DESCRIPTION OF DRAWINGS

[0009] FIG. 1 depicts an example of an environment for training a multi-party machine-learning secure logistic regression model (SLRM) using secure sharing in accordance with implementations of the present specification.

[0010] FIG. 2A depicts an example of a sub-process for iteratively updating parameters of an SLRM in accordance with implementations of this specification.

[0011] FIG. 2B depicts an example of a sub-process for iteratively updating parameters of an SLRM in accordance with implementations of this specification.

[0012] FIG. 3 depicts an example of a sub-process for iteratively updating parameters of an SLRM in accordance with implementations of this specification.

[0013] FIG. 4A depicts an example of a sub-process for iteratively updating parameters of an SLRM in accordance with implementations of this specification.

[0014] FIG. 4B depicts an example of a sub-process for iteratively updating parameters of an SLRM in accordance with implementations of this specification.

[0015] FIG. 5 depicts an example of a process for determining whether to terminate iterations of updating parameters of an SLRM in accordance with implementations of this specification.

[0016] FIG. 6 depicts an example of a process for training a multi-party SLRM using an event-driven interactive secure modeling procedure in accordance with implementations of this specification.

[0017] FIG. 7 depicts an example of a process that can be executed in accordance with implementations of the present specification.

[0018] FIG. 8 depicts an example of a process that can be executed in accordance with implementations of the present specification.

[0019] FIG. 9 depicts an example of a diagram illustrating modules of an apparatus in accordance with implementations of the specification

[0020] Like reference numbers and designations in the various drawings indicate like elements.

DETAILED DESCRIPTION

[0021] The following detailed description describes training a secure logistic regression model (SLRM) based on secret sharing, and is presented to enable any person skilled in the art to make and use the disclosed subject matter in the context of one or more particular implementations. Various modifications, alterations, and permutations of the disclosed implementations can be made and will be readily apparent to those of ordinary skill in the art, and the general principles defined may be applied to other implementations and applications, without departing from the scope of the specification. In some instances, details unnecessary to obtain an understanding of the described subject matter may be omitted so as to not obscure one or more described implementations with unnecessary detail and inasmuch as such details are within the skill of one of ordinary skill in the art. This specification is not intended to be limited to the described or illustrated implementations, but to be accorded the widest scope consistent with the described principles and features.

[0022] Logistic regression is a generalized linear regression and is one type of classification and prediction algorithms. A logistic regression algorithm estimates discrete values from a series of known dependent variables and estimates the probability of the occurrence of an event by

fitting the data into a logic function. Logistic regression can be used for classification (e.g., spam email classification), credit risk calculation, and other applications.

[0023] Large data sets including information about consumers can be leveraged to provide understanding of consumer habits, targets for marketing campaigns, and other applications. Some organizations have established cooperative data labs to build a secure data training model and to facilitate data exchange between organizations. During the data cooperation process, a machine learning model is built based on data obtained from different participating organizations.

[0024] To address privacy concerns related to the sharing of consumer data, the cooperating organizations may use various methods to ensure that their private consumer data is not exposed to the other cooperating organizations during the training of the model. For example, the consumer data can be encrypted using homomorphic encryption techniques. Because the encryption is homomorphic, the model training will produce encrypted results that, when decrypted, will match the training results that would be obtained from training with the unencrypted training data. The output results of the model training are returned to the participating parties so that they can decrypt and obtain the final results.

[0025] Various problems exist in the current data cooperation technologies. For example, under the current approach, each party needs to expose its own (possibly highly sensitive) data to other parties, creating a risk of data leakage. In addition, although many data labs have implemented techniques such as cloud computing, multi-tenant separation, data desensitization, data auditing, and other techniques to ensure data privacy, parties still have no guarantee that their data is being kept secure. As such, the selection of a participating party or a neutral third party to aggregate data and process the aggregated data can be difficult due to the lack of trust between the parties. Further, because there are no generally accepted standards or guidelines for data cooperation, so each party may have to develop their own standards, which may be time consuming and expensive. In addition, a machine learning scheme based on homomorphic encryption or differential privacy is computationally inefficient and thus may require a large amount of processing power, leading to increased costs. Further, traditional modeling tools and processes, although powerful, are demanding for modelers and requires significant time and effort to build the training models.

[0026] Implementations of this specification introduce a new approach of training SLRMs by using secret sharing and an event-driven interactive secure modeling procedure. The described

implementations describe techniques by which an SLRM can be iteratively updated by feeding training data received from both parties.

[0027] The SLRM is trained by providing training data to the model. The sources of the training data are independent secure computation nodes (SCNs), and each SCN keeps its training data secret from other nodes using a secret sharing scheme. As previously described, since the training data may be supplied by different SCNs controlled by different entities, securing the training data for sharing between the SCNs becomes important so any sensitive information in the training data is not revealed to an entity other than the one providing the training data. Specifically, to consolidate such cooperation, the described techniques introduce random numbers to enable each SCN to protect its private training data from the other SCNs.

[0028] In addition, the sharing of training data between the SCNs can be controlled by an event-driven integrative secure modeling procedure. In some implementations, the event-driven interactive secure modeling procedure is based on an event-driven model (or so-called “publish-subscribe” model). This model can separate parties who rely on each other to complete its own task. By using this model, both parties can focus on its own service process. One party (the “publisher”) sends a notice when its service process is completed. The other party (the “subscriber”) monitors for the notification, and once the notification is received, its service process can be triggered accordingly. During the training process, each SCN maintains a message queue to receive data from the other party and in response, triggers corresponding modeling steps to carry on the SLRM.

[0029] The described techniques can have a variety of applications. For example, the techniques can be applied in data cooperation between financial institutions, financial institutions and a government entity, or other organizations.

[0030] In some implementations, the disclosed framework uses an SLRM and a secret sharing scheme. The secret sharing scheme is a type of encryption used in scenarios involving multi-party collaboration. In a secret sharing scheme, a secret (e.g., an encryption key or data set) is divided to several different shares in a predetermined manner, and each share is provided to a different participating party. The secret cannot be recovered or restored by a single participating party, in this way, the secrecy and security of the secret are ensured. For the purpose of this specification, the algorithm used protect the training used by the SLRM is not limited to secret sharing. Compared with homomorphic encryption, the overall computational efficiency is

greatly improved by using secret sharing. Further because the raw training data is not transformed, the training process is an accurate computation based on the raw training data, and the output model result of the training is an accurately trained model based on the raw training data.

[0031] In some implementations, a distributed model training framework is implemented and the framework introduces an independent third-party random number service. In these implementations, before any raw data is input to the training model, it goes through a computation process in conjunction with the random numbers generated and distributed by the third-party random number service. In such implementations, an event-driven interactive secure procedure is further adopted to improve the efficiency of the distributed model. In this way, information leakage of the raw data can be prevented, and the integrity of the modeling result and the precision of the model are ensured.

[0032] FIG. 1 depicts an example of an environment 100 for training a multi-party machine-learning secure logistic regression model (SLRM) using secret sharing in accordance with implementations of the present specification. The data cooperation service can be carried out by one or more servers that provide organizations with a platform/environment for data cooperation. The example environment 100 includes a user 102, a security management agent 104, a node management agent 106, a random number provider 108, a network 110, and at least two secure computation nodes (SCN) SCN A 112 and SCN B 114. The example environment 100 can include additional users, secure computation node computers, networks, systems, or other components. The environment 100 can be configured in another manner in some implementations.

[0033] In some implementations, the network 110 includes a local area network (LAN), wide area network (WAN), the Internet, or a combination of these or other networks. The network 110 can include one or more of a wireless network or wireline networks. The network 110 connects computing devices (e.g., the servers 104-108) and secure computation nodes (e.g., the SCNs 112, 114). In some implementations, the network 110 can be accessed over a wired and/or a wireless communications link.

[0034] In some cases, prior to the start of the training process, a user 102 can predetermine various parameters and settings associated with the SLRM. These parameters may include, for example, the size of the training data, features of the training data and corresponding data processing settings, or a hyperparameter (i.e., a parameter of a prior distribution) of the model.

After initializing the model settings, information associated with the model is sent to the security management agent 104, which can subsequently coordinate with the SCNs to complete the specific modeling logic.

[0035] In some implementations, the security management agent 104 and the node management agent 106 can be integrated as a single component to manage and control the modeling process, as well as the SCNs (e.g., 112, 114) participating in the process. The security management agent 104 and the node management agent 106 may also be separate components, as shown in FIG. 1.

[0036] In some implementations, the security management agent 104 may be configured to manage training of the SLRM, including configuration, modeling, iterative computation, and process management of the training model. Specifically, the security management agent 104 can facilitate the modeling process jointly carried out by the SCNs 112, 114, including, for example, initializing each iteration cycle, and determining whether the training model is converged after a number of iteration circles. In addition, the security management agent 104 can also obtain specific data structure and other information associated with the training data from each SCN. For example, obtaining information such as the source of training data, features of the training data (e.g., the number of rows and columns of each training data set).

[0037] In some implementations, the node management agent 106 can be configured to perform node selection, node management, project data management, etc. For example, once the security management agent 104 received modeling requests from SCN A 112 and SCN B 114, and collected corresponding data information of SCNs A and B, the node management agent 106 can inform, through the security management agent 104, each SCN that the identity of other SCN(s) it needs to work with, the location to obtain additional training data, and distribute corresponding parameters to each SCN participate in the training process. In addition, the node management agent 106 also notifies SCNs A and B of the location of the random number provider 108.

[0038] In the depicted example, the SCN A 112 and SCN B 114 can be operated by separate organizations possessing data sets about their separate users seeking to facilitate data exchange or data cooperation with each other. For example, the organizations operating SCN A 112 and SCN B 114 may possess training data sets P0 and P1, respectively, with both P0 and P1 being inputs to a machine learning model. The output result of the training model can be, for example,

a prediction result that can be used by both SCN A 112 and SCN B 114 to carry out a certain service, such as, a prediction of the risk of issuing a loan to a customer of SCN A 112 or SCN B 114. After SCNs A 112 and B 114 received the model parameters and settings from the security management agent 104, they need to complete the modeling task through network communications with each other. For security purpose, especially in cases where the training data owned by each SCN is highly sensitive privacy data, SCNs A 112 and B 114 can hide or obfuscate portions of the training data from each other. To obfuscate the training data, SCNs A 112 and B 114 can request random numbers from the random number provider 108, and perform computations using its own training data and the received random numbers (for example, addition or multiplication of the random numbers and portions of the data). The random numbers can be used to provide data obfuscation or encryption of the training data. In some cases, only portions of the training data containing highly sensitive privacy data (e.g., personal information of users) can be obfuscated or encrypted, thereby allowing the other party to use the non-sensitive portions of the data for training while not allowing the other party access to the highly sensitive privacy data. Any suitable encryption scheme can be used, such as RSA, DES/TripleDES, and other well-known encryption schemes. In some implementations, the random number can be a number, a vector, or a matrix, etc. In some implementations, the random number can be generated by either SCN 112, 114. In some implementations, the random numbers can be provided by an independent third party to ensure that no private data can be revealed by the other SCN during sharing and training. In some implementations, services related to the random number provider 108, security management agent 104, and node management agent 106 can be provided and performed by a mutual selected and trusted third party agent.

[0039] For each SCN, after the data is encrypted by using the random numbers, the encrypted data can be sent to the other SCN. Because data transmitted between the SCNs 112, 114 is encrypted, sensitive information of the data is not exposed. In some implementations, computations results from SCNs A and B 112, 114 are used for the machine learning model training. Specifically, each SCN uses the received encrypted data as inputs to the SLRM, to iteratively update the parameter of the logistic regression function that the SLRM is based. After a number of iterations, the training may be terminated based on a predetermined condition. In some implementations, local data management is performed by each SCN 112, 114, and may

include storage of data in a database, object store, an in-memory data store (e.g., Redis), or other type of storage.

[0040] FIG. 2A depicts an example of a sub-process 200a for iteratively updating parameters of an SLRM in accordance with implementations of this specification.

[0041] In the depicted example, to optimize an objective function of the SLRM, a mini batch Stochastic Gradient Descent (SGD) method is used. SGD is an iterative method for optimizing a differentiable objective function based on a stochastic approximation of gradient descent optimization. In this specification, to optimize the objective function, the SGD method would perform the following iterations:

$$\theta[j] := \theta[j] - \frac{\alpha}{m} \sum_{i=1}^m (\text{sigmoid}(X_i \cdot \theta) - Y_i) X_i[j] - \frac{\lambda}{m} \theta[j]$$

eq. 1

where m represents the sample size of the mini batch SGD. In this example, X is an m*k sample matrix. Each row of the matrix X represents a sample, and X_i represents the i^{th} row of the matrix X, $[j]$ represents the j^{th} element of vector X_i . θ represents a parameter column vector. Y_i represents the label of the i^{th} sample of the mini batch samples, where Y_i can be 0 or 1. α and λ are hyperparameters that determine a machine learning network structure and how the network is trained. They can be set before training and by a user.

[0042] In this depicted example, by using secret sharing, all sample training data sets used in the equation (1) are divided to two shares. That is, the sample training data for the SLRM comes from two sources, SCN P_0 and SCN P_1 . Specifically, the sample data matrix X is divided to X^L and X^R , so the sample data X^L belong to SCN P_0 , while X^R belong to SCN P_1 . Assume that the samples data in SCN P_0 and SCN P_1 has features k_0 and k_1 , respectively, and $k = k_0 + k_1$. For a sample data set X_i , SCN P_0 contains elements of X_i , expressed as $X_i[1], X_i[2], \dots, X_i[k_0]$, while SCN P_1 contains elements of X_i , expressed as $X_i[k_0 + 1], X_i[k_0 + 2], \dots, X_i[k]$. Likewise, the parameter column vector θ can also be divided into θ^L and θ^R . As such, using these redefined parameters, under the vertical data division, equation (1) can be expressed as:

$$\theta[j] := \theta[j] - \frac{\alpha}{m} \sum_{i=1}^m (\text{sigmoid}(X_i^L \cdot \theta^L + X_i^R \cdot \theta^R) - Y_i) X_i[j] - \frac{\lambda}{m} \theta[j]$$

eq. 2

Where X and Y are the input data to be protected. X represents feature data and Y represents a predication made based on the feature data. For example, in a loan-borrowing scenario, X can be the income, education history, credit history, etc. Based on the information, the bank can make a prediction Y , which is whether the risk of the loan borrower is low enough to issue the loan. Θ is an interim result that needs to be protected, and after the training process terminated, Θ is also a final output of the training result. Other parameters listed in equation (2) are well-known parameters that routinely used.

[0043] The secure logistic regression training algorithm used in the SLRM is based on a mini batch SGD that has a second order regularization, and applies the mathematic circuit (A) and the Garbled Circuit (Yao) of the two-party ABY secured computation framework. The mathematic circuit (A) is based on a multiplication triple and secret sharing, and can be used to calculate addition, subtraction, and multiplication, therefore can compute polynomial, dot product, and matrix multiplications that are used in the algorithm. Meanwhile, the Gabled Circuit (Yao) can be used to perform other types of calculations. In this computational framework, each SCN uses secret sharing for secure calculation. After each computation step, an interim computation result is generated and divided into shares (which may be equal or unequal), while each SCN obtains one share of the interim computation result. After each step, both SCNs enter the next step using the obtained shares, and eventually combine the final generated shares when the iteration terminated.

[0044] Before the iteration loop starts, all parameters used to update the model are first initialized. During the initialization process, both SCNs generate a random column vector as a share of the initialized parameter column vector Θ , where $\dim(\theta) = (k_0+k_1+1, 1)$, $\dim(\theta^L)=(k_0+1, 1)$, $\dim(\theta^R)=(k_1, 1)$. The initialized parameter column vector Θ can be represented by its shares as:

$$\theta^L = \langle \theta^L \rangle_0 + \langle \theta^L \rangle_1$$

eq. 3

$$\theta^R = \langle \theta^R \rangle_0 + \langle \theta^R \rangle_1$$

eq. 4

where $\langle \rangle$ represents a share, and $[i]$ represents the i^{th} element of a vector (that is, $\Theta[i] = \langle \Theta[i] \rangle_0 + \langle \Theta[i] \rangle_1$). Thus, the generated random column vector at SCN P_0 can be expressed as the following equation:

$$\langle \theta \rangle_0 = (\langle \theta[1] \rangle_0, \langle \theta[2] \rangle_0, \langle \theta[3] \rangle_0 \dots \langle \theta[k] \rangle_0) \quad \text{eq. 5}$$

[0045] Because each sample data set is vertically divided, $\langle \theta \rangle_0$ can be further divided by the following two column vectors:

$$\begin{aligned} \langle \theta^L \rangle_0 &= (\langle \theta^L[1] \rangle_0, \langle \theta^L[2] \rangle_0, \langle \theta^L[3] \rangle_0 \dots \langle \theta^L[k_0] \rangle_0) \\ \langle \theta^R \rangle_0 &= (\langle \theta^R[1] \rangle_0, \langle \theta^R[2] \rangle_0, \langle \theta^R[3] \rangle_0 \dots \langle \theta^R[k_1] \rangle_0) \end{aligned} \quad \text{eq. 6}$$

eq. 7

where $\langle \theta \rangle_0 = \langle \theta^L \rangle_0 \parallel \langle \theta^R \rangle_0$, and where $\parallel$ represents a connecting relationship.

[0046] Likewise the generated random column vector at SCN P_1 can be expressed as the following equation:

$$= (\langle \theta[1] \rangle_1, \langle \theta[2] \rangle_1, \langle \theta[3] \rangle_1 \dots \langle \theta[k] \rangle_1)$$

eq. 8

[0047] Because each sample data set is vertically divided, $\langle \theta \rangle_1$ can be further divided by the following two column vectors:

$$\langle \theta^L \rangle_1 = (\langle \theta^L[1] \rangle_1, \langle \theta^L[2] \rangle_1, \langle \theta^L[3] \rangle_1 \dots \langle \theta^L[k_0] \rangle_1)$$

eq. 9

$$\langle \theta^R \rangle_1 = (\langle \theta^R[1] \rangle_1, \langle \theta^R[2] \rangle_1, \langle \theta^R[3] \rangle_1 \dots \langle \theta^R[k_1] \rangle_1)$$

eq. 10

where $\langle \theta \rangle_1 = \langle \theta^L \rangle_1 \parallel \langle \theta^R \rangle_1$, and where $\parallel$ represents a connecting relationship.

[0048] The process of iterations is illustration by FIGS. 2-6. As previously explained, the purpose for the iterations is updating the parameter θ shown in equation (2).

[0049] FIG. 2A illustrates the first sub-step (herein as “step 1.1”) of the first step of the iteration circle (herein as “step 1”) during one iteration. In step 1, each SCN first calculates a share of A based on the equation:

$$A = X\theta = X^L\theta^L + X^R\theta^R$$

eq. 11

where A is calculated by using the mini batch sample vector X multiplied by the column vector of the parameter θ .

[0050] In some implementations, X^L and X^R will also be used for updating parameters in step 3 of the iteration circle. In some implementations, the same mini batch sample data can be used for computation in a later iteration.

[0051] FIG. 2A (step 1.1) illustrates the calculation of the value of $X^L \Theta^L$, using the multiplication triple and secret sharing. As shown in FIG. 2A, SCN P_0 is the party provides the original data. To hide the original data, SCN P_0 and SCN P_1 first obtain random numbers. In some implementations, the random number can be a number, a vector, or a matrix. In some implementation, the random numbers can be generated by SCNs. In some implementations, the random number can be requested and received from a third party agency, for example, the random number provider 108 shown in FIG.1

[0052] As shown in FIG.2A, the obtained random numbers include a random matrix u , a random vector v , and a random number z . The obtained random numbers are distributed between SCN P_0 and SCN P_1 . In some implementations, SCN P_0 obtains a random matrix u , a share of v that expressed as v_0 , a share of z that expressed as z_0 . SCN P_1 obtains a share of v that expressed as v_1 , and a share of z that expressed as z_1 . In some implementations, the shares of z can be generated by a homomorphic calculation. In some implementations, the random vector u is generated by SCN P_0 , while the random vector v 's share v_0 and v_1 are generated by SCN P_0 and SCN P_1 , respectively. In some implementations, u , v , and z and their corresponding shares are all generated by a trusted third party commodity server. Each of the random numbers, and the share of the corresponding random number are interrelated and the relationship among them can be expressed as:

$$z_0 + z_1 = u * v = u * (v_0 + v_1)$$

eq. 12

[0053] Assume $a = X^L$, and $b_0 = \langle \Theta^L \rangle_0$. In order to hide the data of SCN P_0 , encrypts a by using u , for example, by performing an addition, a subtraction or a multiplication of a and u . In some implementation, the random matrix u can be the same when hiding the same X^L in a later iteration. Likewise, $\langle \Theta^L \rangle_0$ is encrypted by using the random vector v_0 . As shown in FIG. 2A, SCN P_0 sends the encrypted X^L (which is expressed as $e = a - u$) and the encrypted $\langle \Theta^L \rangle_0$ (which is expressed as $(b_0 - v_0)$) to SCN P_1 . In some implementations, if the same random matrix u is used to hide the same X^L in a later iteration, the encrypted X^L ($e = a - u$) does not need to be resent. At the SCN P_1 side, assume $b_1 = \langle \Theta^L \rangle_1$. In this case, the random vector share v_1 is used to hide the value of $\langle \Theta^L \rangle_1$, and $(b_1 - v_1)$ is sent from SCN P_1 to SCN P_0 .

[0054] After the data exchange between SCN P_0 and SCN P_1 , the step 1.1 data queue at SCN P_0 is updated as:

$$c_0 = u * f + e * b_0 + z_0 \quad \text{eq. 13}$$

where $f = b - v$

[0055] And the step 1.1 data queue at SCN P_1 is updated as:

$$c_1 = e * b_1 + z_1 \quad \text{eq. 14}$$

where each of c_0 and c_1 is a share of $X^L \Theta^L$,

[0056] Based on the equations above, $X^L \Theta^L$ can be calculated as:

$$X^L \Theta^L = c_0 + c_1 \quad \text{eq. 15}$$

$$c_0 + c_1 = u * f + e * b + u * v \quad \text{eq. 16}$$

$$c_0 + c_1 = u * b - u * v + a * b - u * b + u * v \quad \text{eq. 17}$$

[0057] FIG. 2B depicts an example of a sub-process 200b for iteratively updating parameters of an SLRM in accordance with implementations of this specification.

[0058] Specifically, FIG. 2B shows a second sub-step (herein as step 1.2) of step 1 of the iteration circle. At step 1.2, the value of $X^R \Theta^R$ is calculated using the multiplication triple and secret sharing. As shown in FIG. 2B, SCN P_1 is the party provides the original data. To hide the original data, SCN P_1 and SCN P_0 first obtain random numbers.

[0059] As shown in FIG. 2B, the obtained random numbers include a random matrix u , a random vector v , and a random number z . The obtained random numbers are distributed between SCN P_1 and SCN P_0 . SCN P_1 obtains a random matrix u , a share of v that expressed as v_0 , a share of z that expressed as z_0 . SCN P_0 obtains a share of v that expressed as v_1 , and a share of z that expressed as z_1 . In some implementations, the shares of z can be generated by homomorphic calculation. In some implementations, the random vector u is generated by SCN P_1 , while the random vector v 's share v_0 and v_1 are generated by SCN P_1 and SCN P_0 , respectively. In some implementations, u , v , and z and their share are all generated by a trusted third party commodity server. Each of the random numbers, and the share of the corresponding random number are interrelated and satisfies a relationship as shown in equation (12).

[0060] Assume $a = X^R$, and $b_0 = \langle \Theta^R \rangle_0$, to hide the data information of a , SCN P_1 first encrypt a by u , for example, perform an addition, a subtraction or a multiplication between a and u . In some implementation, the random matrix u can be the same when hiding the same X^R in a later iteration. Likewise, $\langle \Theta^R \rangle_0$ is first encrypted by using the random vector v_0 . As shown

in FIG. 2B, SCN P_1 sends the encrypted X^R (which is expressed as $e = a - u$) and the encrypted $\langle \theta^R \rangle_0$ (which is expressed as $(b_0 - v_0)$) to SCN P_0 . In some implementations, if the same random matrix u is used to hide the same X^L in a later iteration, the encrypted X^L ($e = a - u$) does not need to resend. At the SCN P_0 side, assume $b_1 = \langle \theta^R \rangle_1$. In this case, the random vector share v_1 is used to hide the value of $\langle \theta^R \rangle_1$, and $(b_1 - v_1)$ is sent from SCN P_0 to SCN P_1 .

[0061] After the data exchange between SCN P_1 and SCN P_0 , the step 1.2 data queue at SCN P_1 is updated by equation (13), and the step 1.2 data queue at SCN P_0 is updated by equation (14). Based on the equations above, $X^L \theta^L$ can be calculated by equations (16) and (17), as well as:

$$X^R \theta^R = c_0 + c_1 \quad \text{eq. 18}$$

[0062] As such, step 1 of one iteration circle is completed, and equation (11) can be calculated by combining the results of equations (15) and (18).

[0063] FIG. 3 depicts an example of a sub-process 300 for iteratively updating parameters of an SLRM in accordance with implementations of this specification. Specifically, FIG. 3 illustrates the second step in the iteration cycle (herein referred to as “step 2”).

[0064] At step 2, a column vector of the prediction error is calculated by using an equation:

$$E = g(A) - Y_i \quad \text{eq. 19}$$

Where A is the same value as in equation (11) described in step 1. g is a fitting function of a sigmoid function, which can be a polynomial function fitting. That is, $g()$ can be a polynomial function and its highest order is d . In the depicted example in this specification, set $d=7$, and $g(x)$ can be expressed by the equation:

$$g(x) = 0.5 + 1.73496 * (x/8) - 4.19407 * (x/8)^3 + 5.43402 * (x/8)^5 - 2.50739 * (x/8)^7 \quad \text{eq. 20}$$

where $g(A)$ represents the column vector composed by $g(A[1])$, $g(A[2])$, ..., $g(A[m])$.

[0065] Using the multiplication triple and secret sharing, each of SCN P_0 and SCN P_1 needs to calculate $g(\langle A[i]_0 \rangle + \langle A[i]_1 \rangle)$. Assume $p = \langle A[i]_0 \rangle$, and $q = \langle A[i]_1 \rangle$. The polynomial function $g(p+q)$ can be extended as the function:

$$g(p+q) = h_0(q) + h_1(q)p + h_2(q)p^2 + \dots + h_d(q)p^d \quad \text{eq. 21}$$

Where each of $h_0, h_1, \dots, h_d$ is a polynomial function of q , and can be calculated by SCN P_1 , while $p, p^2, p^3, \dots, p^d$ can be calculated by SCN P_0 .

[0066] Assume vector $a = (p, p^2, p^3 \dots p^d)$, and vector $b = (h_1(q), h_2(q), \dots, h_d(q))$, so $g(p+q) = a \cdot b + h_0(q)$, where the dot product ($a \cdot b$) can be calculated by the process illustrated in FIG. 3, which includes optimized multiplication triple and secret sharing. A final result of E can be calculated by performing addition based on secret sharing.

[0067] As shown in FIG. 3, the obtained random numbers include a random matrix u , a random vector v , and a random number z . The obtained random numbers are distributed between $SCN P_0$ and $SCN P_1$. $SCN P_0$ obtains a random matrix u , a share of z that expressed as z_0 . $SCN P_1$ obtains the random vector v , and a share of z that expressed as z_1 . Each of the random numbers, and the share of the corresponding random number are interrelated and the relationship among them can be expressed as:

$$z_0 + z_1 = u \cdot v \quad \text{eq. 22}$$

[0068] Then, as illustrated in FIG. 3, $SCN P_0$ first sends encrypted data $e = a - u$ to $SCN P_1$, and $SCN P_1$ sends encrypted data $f = b - v$ to $SCN P_0$. The steps and calculations are similar to those in step1, for details please refer to the previous descriptions of FIGS. 2A and 2B.

[0069] After the data exchange between $SCN P_0$ and $SCN P_1$, the step 2 data queue at $SCN P_0$ is updated as:

$$c_0 = u \cdot f + z_0 \quad \text{eq. 23}$$

[0070] And the step 2 data queue at $SCN P_1$ is updated as:

$$c_1 = e \cdot b + z_1 \quad \text{eq. 24}$$

[0071] Based on the equations above, ($a \cdot b$) can be calculated as:

$$(a \cdot b) = c_0 + c_1 \quad \text{eq. 25}$$

$$c_0 + c_1 = u \cdot f + e \cdot b + u \cdot v \quad \text{eq. 26}$$

$$c_0 + c_1 = u \cdot b - u \cdot v + a \cdot b - u \cdot b + u \cdot v \quad \text{eq. 27}$$

[0072] FIG. 4A depicts an example of a sub-process 400a for iteratively updating parameters of an SLRM in accordance with implementations of this specification. FIG. 4B depicts an example of a sub-process 400b for iteratively updating parameters of an SLRM in accordance with implementations of this specification.

[0073] Specifically, FIGS 4A and 4B illustrate the process for performing the third step of one iteration circle (herein as “step3”)

[0074] At step 3, the column vector Θ , and each of the $SCN P_0$ and $SCN P_1$ can obtain a share of the updated Θ . In this step, the updated Θ can be expressed as:

$$\theta := (1 - \frac{\lambda}{m})\theta - \frac{\alpha}{m}X^T E \quad \text{eq. 28}$$

Where E is the same E in equation (19) of step 2, and where

$$X^T E = (X^L)^T E \parallel (X^R)^T E \quad \text{eq. 29}$$

[0075] The method to calculate $(X^L)^T E$ is the same as the method of calculating $X^L \Theta^L$, while the method to calculate $(X^R)^T E$ is the same as the method of calculating $X^R \Theta^R$, and will not be repeated here. In equation (29), X represents a matrix contains feature data of multiple samples, and E represents an error vector.

[0076] After step 3, one iteration circle is completed, and the training process either enters into the next iteration circle and repeats steps 1-3, or the training process is terminated if a condition is satisfied, as described in more details below.

[0077] FIG. 5 depicts an example of a process 500 for determining whether to terminate iterations of updating parameters of an SLRM in accordance with implementations of this specification.

[0078] In some implementations, the iterations can be terminated when the number of completed iteration circles has reached a predetermined number. In some implementations, a threshold is predetermined, and when the difference between two consecutive iteration results is less than that threshold, the iteration is terminated.

[0079] Specifically, for example, assume the parameter before and after one iteration circle is Θ and Θ' , calculate the difference $D = (\Theta' - \Theta)$ using secret sharing. Assume, $a_0 = \langle D^T \rangle_0$, $a_1 = \langle D^T \rangle_1$, $b_0 = \langle D \rangle_0$, and $b_1 = \langle D \rangle_1$. Each of SCN P_0 and SCN P_1 calculates a share of $D^T D$ using multiplication triple and secret sharing, and the combine each result to obtain D.

[0080] As shown in FIG. 5, In some implementations, SCN P_0 generates the random matrix u_0 and v_0 , and SCN P_0 generates the random matrix u_1 and v_1 . The method of subsequent calculation is similar to the methods previously described in FIGS. 2 and 4, and will not be repeated here. After the data exchanged between SCN P_0 and SCN P_1 , computation result at the SCN P_0 is:

$$c_0 = -e * f + a_0 * f + e b_0 + z_0 \quad \text{eq. 30}$$

where $f = b - v$.

[0081] computation result at the SCN P_1 is:

$$c_1 = a_1 * f + eb_1 + z_1 \quad \text{eq. 31}$$

where each of c_0 and c_1 is a share of $D^T D$

[0082] Based on the equations above, $D^T D$ can be calculated as:

$$D^T D = c_0 + c_1 \quad \text{eq. 32}$$

$$c_0 + c_1 = e*f + a*f + e*b + u*v \quad \text{eq. 33}$$

$$c_0 + c_1 = u*f + a*b - u*b + u*v \quad \text{eq. 34}$$

$$c_0 + c_1 = u*b - u*v + a*b - u*b + u*v \quad \text{eq. 35}$$

[0083] FIG. 6 depicts an example of a process 600 for training a multi-party SLRM using an event-driven interactive secure modeling procedure in accordance with implementations of this specification.

[0084] In some implementations, various steps of method 600 can be run in parallel, in combination, in loops, or in any order. For clarity of presentation, the description that follows generally describes method 600 in the context of the other figures in this description. However, it will be understood that method 600 may be performed, for example, by any suitable system, environment, software, and hardware, or a combination of systems, environments, software, and hardware, as appropriate. For example, method 600 can be performed by one or more data processing apparatus that is configured to execute machine learning algorithms using secret sharing. The data processing apparatus can include or be implemented by one or more of, for example, general-purpose CPUs or hardware accelerators such as GPUs, FPGAs, and even custom ASIC processors.

[0085] In some implementations, as illustrated in FIG.6, process 600a (including steps 602a-622a) is performed by the Node A in conjunction with a database, while process 600b (including steps 602b-624b) is performed by the Node B in conjunction with the database. The database can be a Remote Dictionary Server (Redis) and supports the transmission and temporary storage of data for nodes A and B and B. In some implementations, the data can be transmitted between SCNs A and B 112, 114 without going through a database and the subscription queues may be stored and updated locally at each of Node A and Node B. Before the iteration process starts, each of Node A and Node B enters into an independent modeling process and initiate one batch iteration. Each of Node A and Node B can publish and subscribe data, therefore each of Node A and Node B is a publisher (or “producer”) and also a subscriber (or “consumer”). Under the

event-driven model in this example, even Node A and Node B reply on each other, their modeling process 600 a and 600 b are independent and are proceed separately.

[0086] At 602a and 602b, Node A and Node B each enter one independent batch iteration. 602a and 602 b can happen concurrently or consecutively. After 602a, process 600a proceeds to 604 a. After 602b, process 600b proceeds to 604b.

[0087] At 604 a, Node A publishes step 1 data to Node B. In some implementations, the step 1 data is published by sending encrypted sample data to a database, so the database can store and update the subscriber queue. Once Node A completed this step, a notification might be sent to Node B to inform Node B that publishing step 1 data from Node A has completed. After 604a, process 600a proceeds to 606a.

[0088] At 606 a, Node A subscribes to step 1 data from node B. In some cases, because the SLRM is trained based on secret sharing, Node A cannot complete the training itself and both data from Nodes A and B are used as input to the model. In some implementations, Node A makes such subscription by requesting step 1 data from Node B from Node B. If the data queue in the database is updated by step 1 data from Node B, Node A will receive a notification. Because at this time Node A has not received the notification from Node B, the next step of 600a cannot be triggered and process 600a is temporarily suspended.

[0089] Meanwhile, at 604b, Node B publishes step 1 data to Node A. In some implementations, the step 1 data is published by sending encrypted sample data to a database, so the database can store and update the subscriber queue. Once Node B complete this step, a notification might be sent to Node A to inform Node A that step 1 data publishing from Node B has completed. After 604b, process 600b proceeds to 606b.

[0090] At 606 b, Node B subscribes to step 1 data from node B. Because at this time Node A already published step 1 data and Node B has already received notification from Node A, the next step is triggered and after 606b, process 600 b proceeds to 608b.

[0091] At 608b, Node B locally computes a step 1 result by using its own data and step 1 data received from Node A. Equations and detailed steps of this step can be referred to the previously described FIG. 2B. After 608b, process 600b proceeds to 610b.

[0092] Because both steps 610b and 612 b can be independently performed by Node B, Node B can perform these two step together or consecutively without relying on Node A's action. After steps 610b and 612b, the subscriber queue in database is updated by using the step 2 data

published by Node B, and a notification of publishing is sent to Node A. After step 612b, because Node B has not received notification from Node A, the next step cannot be triggered and process 600 b is temporarily suspended.

[0093] Returning to step 606a of process 600a. If at the time Node B already carried out step 604 b, and Node A has already received notifications from Node B, the next step of process 600a is triggered and after 606a, process 600a proceeds to 608a.

[0094] Because steps 608a-612a can be independently performed by Node A without data from Node B, Node A can perform these steps consecutively. After step 610a, the subscriber queue in database is updated by using the step 2 data published by Node A, and a notification of publishing is sent to Node B. After step 612a, if Node B already performed step 610b and Node A received corresponding notification, the next step of 600 a is triggered and the process 600 a proceeds to 614a. Otherwise, process 600a is temporarily suspended until step 610 b is performed.

[0095] Because steps 614a -618a can be independently performed by Node A, Node A can perform these steps consecutively. After steps 614a and 616a, the subscriber queue in database is updated by using the step 3 data published by Node A, and a notification of publishing is sent to Node B. After step 618a, because Node A has not received notification from Node B, process 600a may be temporarily suspended until the notification from Node B is received.

[0096] Returning to process 600b. After step 610 a where Node A published its step 2 data and sent the corresponding notification, the next step of process 600b is triggered and process 600b can proceed to 614b. At 614b, Node B locally compute step 2 result by using its own data and step 2 data received from Node A. Equations and detailed steps of the computation step can be referred to the previously described FIG. 3. After 614b, process 600b proceeds to 616b.

[0097] Because each step of 616b-620b can be independently performed by Node B, Node B can perform these three steps consecutively. At 616b, a value of sigmoid (wx)-y is computed by using equation (20). After steps 618b and 620b, the subscriber queue in database is updated by using the step 3 data published by Node B, and a notification of publishing is sent to Node A. After step 620b, if at the time Node A already performed 616a and e Node B has received notification from Node A, the next step of 600b is triggered and process 600b proceeds to 622b.

[0098] At 622b, Node B locally computes step 3 results using its own data and step 3 data received from Node A. Equations and detailed steps of the computation detailed in the

previously-described FIG. 4B. After 622b, because whether to enter the next iteration is jointly determined by Node A and Node B, after 622b, and because Node B has not received notification from Node B, process 600b is temporarily suspended.

[0099] Returning to process 600a, after step 618b where Node B has published its step 3 data and sent the corresponding notification, the next step of process 600a is triggered and process 600a can proceed to 620a. At 620a, Node A locally computes step 3 result by using its own data and step 3 data received from Node A. Equations and detailed steps of the computation step can be referred to the previously described FIG. 3. After 620a, both Node A and Node B have completed an iteration circle.

[0100] As previously described in FIG.4, whether to terminate the iteration circle depends on whether a predetermined condition is satisfied. If so, both processes 600a and 600b proceed to 622a and 624a, and repeat the steps from 602a-620a, and 602b-622b again. If not, the iteration is terminated and both processes 600a and 600b stop at 618a and 622b, respectively.

[0101] FIG. 7 depicts an example of a process 700 that can be executed in accordance with implementations of the present specification. In some implementations, various steps of method 700 can be run in parallel, in combination, in loops, or in any order. For clarity of presentation, the description that follows generally describes method 700 in the context of the other figures in this description. However, it will be understood that method 700 may be performed, for example, by any suitable system, environment, software, and hardware, or a combination of systems, environments, software, and hardware, as appropriate. For example, the method 700 can be performed by one or more data processing apparatus that is configured to execute machine learning algorithms using secret sharing. The data processing apparatus can include or be implemented by one or more of, for example, general-purpose CPUs or hardware accelerators such as GPUs, FPGAs, and even custom ASIC processors.

[0102] At 702, sample training data for an SLRM is divided to two shares using secret sharing, and each share is distributed to an SCN. In some implementations, a sample data matrix X is divided to X^L and X^R , and the sample data matrix X^L belongs to an SCN 1, and the sample data matrix X^R belongs to SCN 2. After 702, process 700 proceeds to 704.

[0103] At 704, parameters of the SLRM are iteratively updated using each share of the sample training data. In some implementations, an objective function of the SLRM is optimized by using a mini batch Stochastic Gradient Descent (SGD) method.

[0104] In some implementations, the SLRM is based on a logistic regression function that can be expressed as :

$$\theta[j] := \theta[j] - \frac{\alpha}{m} \sum_{i=1}^m (\text{sigmoid}(X_i^L \cdot \theta^L + X_i^R \cdot \theta^R) - Y_i) X_i[j] - \frac{\lambda}{m} \theta[j]$$

where m represents the sample size of the mini batch SGD. X represents an m*k sample matrix. Each row of the matrix X represents a sample, and X_i represents the i^{th} row of the matrix X, $[j]$ represents the j^{th} element of vector X_i . The sample data matrix X is divided to X^L and X^R , and the sample data X^L belong to SCN P_0 , while X^R belong to SCN P_1 . θ represents a parameter column vector, and the column vector θ can be vertically divided to θ^L and θ^R .

[0105] In some implementations, training the SLRM includes using an event-driven model. After 704, process 700 proceeds to 706.

[0106] At 706, for each SCN, a share of A is calculated based on:

$$A = X\theta = X^L\theta^L + X^R\theta^R$$

[0107] In some implementations, calculating $X^L\theta^L$ and $X^R\theta^R$ includes, hiding original data provided from each SCN by using random numbers, and exchanging hided data between SCNs. In some implementations, prior to hiding the original data, random numbers are obtained by each SCN. In some implementations, the random number can be a number, a vector, or a matrix. In some implementation, the random numbers can be generated by the SCN. In some implementations, the random number can be requested and received from a third party agency. After 706, process 700 proceeds to 708.

[0108] At 708, a column vector of a prediction error is calculated based on:

$$E = g(A) - Y_i$$

where g is a fitting function of a sigmoid function, which can be a polynomial function fitting. In some implementations, if the order of g(x) is 7, g(x) can be expressed by the equation:

$$g(x) = 0.5 + 1.73496 * (x/8) - 4.19407 * (x/8)^3 + 5.43402 * (x/8)^5 - 2.50739 * (x/8)^7$$

where g(A) represents the column vector composed by g(A[1]), g(A[2]), ... g(A[m]).

After 708, process 700 proceeds to 710.

[0109] At 710, the updated column vector θ can be expressed as:

$$\theta := (1 - \frac{\lambda}{m})\theta - \frac{\alpha}{m} X^T E$$

where $X^T E = (X^L)^T E + (X^R)^T E$

After 710, process 700 proceeds to 712.

[0110] At 712, the iteration is terminated if a predetermined condition is satisfied. In some implementations, the iterations can be terminated when the number of completed iteration cycles has reached a predetermined number.

[0111] In some implementations, a threshold is predetermined, and when the difference between two consecutive iteration results is less than that threshold, the iteration is terminated. After 712, process 700 can stop.

[0112] FIG. 8 depicts an example of a process 800 that can be executed in accordance with implementations of the present specification. In some implementations, various steps of method 700 can be run in parallel, in combination, in loops, or in any order. For clarity of presentation, the description that follows generally describes method 800 in the context of the other figures in this description. However, it will be understood that method 800 may be performed, for example, by any suitable system, environment, software, and hardware, or a combination of systems, environments, software, and hardware, as appropriate. For example, method 800 can be performed by one or more data processing apparatus that is configured to execute machine learning algorithms using secret sharing. The data processing apparatus can include or be implemented by one or more of, for example, general-purpose CPUs or hardware accelerators such as GPUs, FPGAs, and even custom ASIC processors.

[0113] At 802, the SLRM is initialized by a user by determining a number of parameters associated with the SLRM. In some implementations, the parameters can include the size of training data, features associated with the training data, corresponding to settings of the SLRM, hyperparameters of the SLRM.

[0114] In some implementations, after the user has initialized the SLRM, information associated with the SLRM is sent to a security management agent. In some implementations, the security management agent processes the SLRM and training data fed to the model. In some implementations, a node management agent is configured to select and manage SCNs that participate in the training. In some implementations, both of the security management agent and the node management agent can be configured as a third party agent. After 802, process 800 proceeds to 804.

[0115] At 804, random numbers are requested by at least two SCNs from a random number provider, and the requested random numbers are used to encrypt data stored in each SCN. In

some implementations, the random number can be a number, a vector, or a matrix, etc. In some implementations, the random numbers can be generated by at least one SCN. In some implementations, the random numbers can be provided by an independent third party.

[0116] In some implementations, encrypting the data includes performing computations using the data and the received random numbers. In some implementations, the computations performed is at least one of addition, subtraction, and multiplication. After 802, process 800 proceeds to 804.

[0117] At 806, the encrypted data is used as input to iteratively update parameters of an SLRM based on secret sharing. Details of this step will be further described in FIG. 7. After 806, process 800 proceeds to 808.

[0118] At 808, the output of the trained SLRM is used to perform a service for each SCN. In some implementations, the service can be a prediction service or a classification service. After 808, process 800 stops.

[0119] FIG. 9 depicts an example of a diagram 900 illustrating modules of an apparatus in accordance with implementations of the specification. The apparatus 900 can be an example implementation of an apparatus for training multi-party secure logistic regression models. The apparatus 900 can correspond to the implementations described above, and the apparatus 900 includes the following: a divider or dividing unit 902 for dividing sample training data for a secure logistic regression model (SLRM) into a plurality of shares using secret sharing (SS), wherein each share is distributed to a secure computation node (SCN); an updater or updating unit 904 for iteratively updating parameters associated with the SLRM using each share of the sample training data, wherein the iterative updating continues until the occurrence of a predetermined condition; and an outputter or output unit 906 for outputting a training result configured for use by each SCN after iteratively updating the parameters associated with the SLRM.

[0120] In an optional implementation, an objective function of the SLRM is a logistic regression function that is optimized by using a mini batch Stochastic Gradient Descent (SGD) method, and wherein the logistic regression function is expressed as equation (2).

[0121] In an optional implementation, the updater or updating unit 904 is used to perform iteratively updating parameters associated with the SLRM according to an event-driven model.

[0122] In an optional implementation, the updater or updating unit 904 is used to: for each SCN, calculating a value of A representing a column vector, where the calculating is performed based on the equation (11); determining a column vector of a prediction error based on the equation (19); and determining an updated column vector based on equations (28) and (29).

[0123] In an optional implementation, calculating a share of A representing a column vector includes encrypting original data provided by each SCN by using random numbers, and exchanging the encrypted data between the SCNs.

[0124] In an optional implementation, each of the random numbers is at least one of a number, a vector, or a matrix.

[0125] In an optional implementation, the predetermined condition is an occurrence of a difference between two consecutive iteration results that is less than a predetermined threshold.

[0126] The system, apparatus, module, or unit illustrated in the previous implementations can be implemented by using a computer chip or an entity, or can be implemented by using a product having a certain function. A typical implementation device is a computer, and the computer can be a personal computer, a laptop computer, a cellular phone, a camera phone, a smartphone, a personal digital assistant, a media player, a navigation device, an email receiving and sending device, a game console, a tablet computer, a wearable device, or any combination of these devices.

[0127] For an implementation process of functions and roles of each unit in the apparatus, references can be made to an implementation process of corresponding steps in the previous method. Details are omitted here for simplicity.

[0128] Because an apparatus implementation basically corresponds to a method implementation, for related parts, references can be made to related descriptions in the method implementation. The previously described apparatus implementation is merely an example. The units described as separate parts may or may not be physically separate, and parts displayed as units may or may not be physical units, may be located in one position, or may be distributed on a number of network units. Some or all of the modules can be selected based on actual demands to achieve the objectives of the solutions of the specification. A person of ordinary skill in the art can understand and implement the implementations of the present application without creative efforts.

[0129] Referring again to FIG. 9, it can be interpreted as illustrating an internal functional module and a structure of an apparatus for training multi-party secure logistic regression models. The execution apparatus can be an example of an apparatus configured to enable modeling training.

[0130] Implementations of the subject matter and the actions and operations described in this specification can be implemented in digital electronic circuitry, in tangibly-embodied computer software or firmware, in computer hardware, including the structures disclosed in this specification and their structural equivalents, or in combinations of one or more of them. Implementations of the subject matter described in this specification can be implemented as one or more computer programs, e.g., one or more modules of computer program instructions, encoded on a computer program carrier, for execution by, or to control the operation of, data processing apparatus. The carrier may be a tangible non-transitory computer storage medium. Alternatively, or in addition, the carrier may be an artificially-generated propagated signal, e.g., a machine-generated electrical, optical, or electromagnetic signal, that is generated to encode information for transmission to suitable receiver apparatus for execution by a data processing apparatus. The computer storage medium can be or be part of a machine-readable storage device, a machine-readable storage substrate, a random or serial access memory device, or a combination of one or more of them. A computer storage medium is not a propagated signal.

[0131] The term “data processing apparatus” encompasses all kinds of apparatus, devices, and machines for processing data, including by way of example a programmable processor, a computer, or multiple processors or computers. Data processing apparatus can include special-purpose logic circuitry, e.g., an FPGA (field programmable gate array), an ASIC (application-specific integrated circuit), or a GPU (graphics processing unit). The apparatus can also include, in addition to hardware, code that creates an execution environment for computer programs, e.g., code that constitutes processor firmware, a protocol stack, a database management system, an operating system, or a combination of one or more of them.

[0132] A computer program, which may also be referred to or described as a program, software, a software application, an app, a module, a software module, an engine, a script, or code, can be written in any form of programming language, including compiled or interpreted languages, or declarative or procedural languages; and it can be deployed in any form, including as a stand-alone program or as a module, component, engine, subroutine, or other unit suitable

for executing in a computing environment, which environment may include one or more computers interconnected by a data communication network in one or more locations.

[0133] A computer program may, but need not, correspond to a file in a file system. A computer program can be stored in a portion of a file that holds other programs or data, e.g., one or more scripts stored in a markup language document, in a single file dedicated to the program in question, or in multiple coordinated files, e.g., files that store one or more modules, sub-programs, or portions of code.

[0134] The processes and logic flows described in this specification can be performed by one or more computers executing one or more computer programs to perform operations by operating on input data and generating output. The processes and logic flows can also be performed by special-purpose logic circuitry, e.g., an FPGA, an ASIC, or a GPU, or by a combination of special-purpose logic circuitry and one or more programmed computers.

[0135] Computers suitable for the execution of a computer program can be based on general or special-purpose microprocessors or both, or any other kind of central processing unit. Generally, a central processing unit will receive instructions and data from a read-only memory or a random access memory or both. Elements of a computer can include a central processing unit for executing instructions and one or more memory devices for storing instructions and data. The central processing unit and the memory can be supplemented by, or incorporated in, special-purpose logic circuitry.

[0136] Generally, a computer will also include, or be operatively coupled to receive data from or transfer data to one or more mass storage devices. The mass storage devices can be, for example, magnetic, magneto-optical, or optical disks, or solid state drives. However, a computer need not have such devices. Moreover, a computer can be embedded in another device, e.g., a mobile telephone, a personal digital assistant (PDA), a mobile audio or video player, a game console, a Global Positioning System (GPS) receiver, or a portable storage device, e.g., a universal serial bus (USB) flash drive, to name just a few.

[0137] To provide for interaction with a user, implementations of the subject matter described in this specification can be implemented on, or configured to communicate with, a computer having a display device, e.g., a LCD (liquid crystal display) monitor, for displaying information to the user, and an input device by which the user can provide input to the computer, e.g., a keyboard and a pointing device, e.g., a mouse, a trackball or touchpad. Other kinds of

devices can be used to provide for interaction with a user as well; for example, feedback provided to the user can be any form of sensory feedback, e.g., visual feedback, auditory feedback, or tactile feedback; and input from the user can be received in any form, including acoustic, speech, or tactile input. In addition, a computer can interact with a user by sending documents to and receiving documents from a device that is used by the user; for example, by sending web pages to a web browser on a user's device in response to requests received from the web browser, or by interacting with an app running on a user device, e.g., a smartphone or electronic tablet. Also, a computer can interact with a user by sending text messages or other forms of message to a personal device, e.g., a smartphone that is running a messaging application, and receiving responsive messages from the user in return.

[0138] While this specification contains many specific implementation details, these should not be construed as limitations on the scope of what is being claimed, which is defined by the claims themselves, but rather as descriptions of features that may be specific to particular implementations. Certain features that are described in this specification in the context of separate implementations can also be realized in combination in a single implementation. Conversely, various features that are described in the context of a single implementations can also be realized in multiple implementations separately or in any suitable subcombination. Moreover, although features may be described above as acting in certain combinations and even initially be claimed as such, one or more features from a claimed combination can in some cases be excised from the combination, and the claim may be directed to a subcombination or variation of a subcombination.

[0139] Similarly, while operations are depicted in the drawings and recited in the claims in a particular order, this should not be understood as requiring that such operations be performed in the particular order shown or in sequential order, or that all illustrated operations be performed, to achieve desirable results. In certain circumstances, multitasking and parallel processing may be advantageous. Moreover, the separation of various system modules and components in the implementations described above should not be understood as requiring such separation in all implementations, and it should be understood that the described program components and systems can generally be integrated together in a single software product or packaged into multiple software products.

[0140] Particular implementations of the subject matter have been described. Other implementations are within the scope of the following claims. For example, the actions recited in the claims can be performed in a different order and still achieve desirable results. As one example, the processes depicted in the accompanying figures do not necessarily require the particular order shown, or sequential order, to achieve desirable results. In some cases, multitasking and parallel processing may be advantageous.

CLAIMS

What is claimed is:

1. A computer-implemented method for training multi-party secure logistic regression models, comprising:

dividing, by one or more processors, sample training data for a secure logistic regression model (SLRM) into a plurality of shares using secret sharing (SS) comprising hiding original data by encrypting the original data using random numbers generated by a plurality of secure computation nodes (SCN), such that the original data cannot be recovered by using a single share of the plurality of shares, wherein the sample training data is originating from the plurality of secure computation nodes configured to both produce and consume training data;

transmitting, by the one or more processors, each share to one of the plurality of secure computation nodes;

generating, by the one or more processors, updated parameters by iteratively updating current parameters associated with the SLRM using each share of the sample training data, wherein the iterative updating comprises:

for each SCN, calculating a value of A representing a column vector, wherein the calculating is performed based on the following equation:

$$A = X\Theta = X^L\Theta^L + X^R\Theta^R$$

wherein: $X^L\Theta^L$ and $X^R\Theta^R$ each represents a share of A for a SCN,

wherein calculating $X^L\Theta^L$ and $X^R\Theta^R$ comprises hiding original data provided from each SCN by using random numbers, and exchanging the hided data between the SCNs;

a predetermined iteration condition is satisfied; and

after iteratively updating the parameters associated with the SLRM, outputting a training result configured for use by each SCN of the plurality of secure computation nodes.

2. The computer-implemented method of claim 1, wherein an objective function of the SLRM is a logistic regression function that is optimized by using a mini batch Stochastic Gradient Descent (SGD) method, and wherein the logistic regression function is expressed as:

$$\theta[j] := \theta[j] - \frac{\alpha}{m} \sum_{i=1}^m (\text{sigmoid}(X_i^L \cdot \theta^L + X_i^R \cdot \theta^R) - Y_i) X_i[j] - \frac{\lambda}{m} \theta[j]$$

wherein:

α and λ comprising hyperparameters that determine a structure of a machine learning network;

m represents a sample size of the mini batch SGD;

X represents a $m \times k$ sample matrix;

each row of the matrix X represents a sample;

X_i represents an i^{th} row of the matrix X ;

$[j]$ represents a j^{th} element of vector X_i ;

X^L represents a share of the sample data X that belongs to a respective SCN;

X^R represents a share of the sample data X that belongs to the respective SCN; and

θ represents a parameter column vector that is vertically dividable into θ^L and θ^R .

3. The computer-implemented method of claim 1, wherein iteratively updating parameters associated with the SLRM is performed according to an event-driven model.

4. The computer-implemented method of claim 1, wherein iteratively updating parameters associated with the SLRM comprises:

determining a column vector of a prediction error based on the following equation:

$$E = g(A) - Y_i;$$

wherein:

g represents a fitting function of a sigmoid function, the fitting function comprising a polynomial fitting function; and

determining a updated column vector based on equation:

$$\theta := (1 - \frac{\lambda}{m})\theta - \frac{\alpha}{m}X^T E$$

wherein:

$$X^T E = (X^L)^T E || (X^R)^T E,$$

wherein:

α and λ comprising hyperparameters that determine a structure of a machine learning network;

m represents a sample size of a mini batch Stochastic Gradient Descent (SGD) method;

X represents a $m \times k$ sample matrix;

each row of the matrix X represents a sample;

X_i represents an i^{th} row of the matrix X ;

$[j]$ represents a j^{th} element of vector X_i ;

X^L represents a first share of the sample data X that belongs to a first SCN of the plurality of secure computation nodes;

X^R represents the second share of the sample data X that belongs to a second SCN of the plurality of secure computation nodes;

Y represents a prediction value;

Y_i represents a label of the i^{th} sample of the mini batch SGD method;

E represents an error vector;

R , L , and T represent indexes of the shares of a respective SCN; and

Θ represents a parameter column vector, and the column vector that is vertically dividable into Θ^L and Θ^R .

5. The computer-implemented method of claim 4, wherein calculating a share of A representing a column vector comprises:

encrypting original data provided by each SCN by using random numbers, and
exchanging the encrypted data between the plurality of secure computation
nodes.

6. The computer-implemented method of claim 5, wherein each of the random numbers is at least one of a number, a vector, or a matrix.

7. The computer-implemented method of claim 6, wherein the predetermined iteration condition is an occurrence of a difference between two consecutive iteration results that is less than a predetermined threshold.

8. A non-transitory, computer-readable medium storing one or more instructions executable by a computer system to perform operations comprising:

dividing sample training data for a secure logistic regression model (SLRM) into a plurality of shares using secret sharing (SS) comprising hiding original data by encrypting the original data using random numbers generated by a plurality of secure computation nodes, such that the original data cannot be recovered by using a single share of the plurality of shares, wherein the sample training data is originating from the plurality of secure computation nodes configured to both produce and consume training data;

transmitting each share to one of the plurality of secure computation nodes;

generating updated parameters by iteratively updating current parameters associated with the SLRM using each share of the sample training data, wherein the iterative updating comprises:

for each SCN, calculating a value of A representing a column vector, wherein the calculating is performed based on the following equation:

$$A = X\Theta = X^L\Theta^L + X^R\Theta^R$$

wherein: $X^L\Theta^L$ and $X^R\Theta^R$ each represents a share of A for a SCN,

wherein calculating $X^L\Theta^L$ and $X^R\Theta^R$ comprises hiding original data provided from each SCN by using random numbers, and exchanging the hidden data between the SCNs;

determining that a predetermined iteration condition is satisfied; and

after iteratively updating the parameters associated with the SLRM, outputting a training result configured for use by each SCN of the plurality of secure computation nodes.

9. The non-transitory, computer-readable medium of claim 8, wherein an objective function of the SLRM is a logistic regression function that is optimized by using a mini batch Stochastic Gradient Descent (SGD) method, and wherein the logistic regression function is expressed as:

$$\theta[j] := \theta[j] - \frac{\alpha}{m} \sum_{i=1}^m (\text{sigmoid}(X_i^L \cdot \theta^L + X_i^R \cdot \theta^R) - Y_i) X_i[j] - \frac{\lambda}{m} \theta[j]$$

wherein:

α and λ comprising hyperparameters that determine a structure of a machine learning network;

m represents a sample size of the mini batch SGD;

X represents a m*k sample matrix;

each row of the matrix X represents a sample;

X_i represents an i^{th} row of the matrix X;

[j] represents a j^{th} element of vector X_i ;

X^L represents a share of the sample data X that belongs to a respective SCN;

X^R represents a share of the sample data X that belongs to the respective SCN; and

θ represents a parameter column vector that is vertically dividable into θ^L and θ^R .

10. The non-transitory, computer-readable medium of claim 8, wherein iteratively updating parameters associated with the SLRM is performed according to an event-driven model.

11. The non-transitory, computer-readable medium of claim 8, wherein iteratively updating parameters associated with the SLRM comprises:

determining a column vector of a prediction error based on the following equation:

$$E = g(A) - Y_i;$$

wherein:

g represents a fitting function of a sigmoid function, the fitting function comprising a polynomial fitting function; and

determining a updated column vector based on equation:

$$\theta := (1 - \frac{\lambda}{m})\theta - \frac{\alpha}{m}X^T E$$

wherein:

$$X^T E = (X^L)^T E || (X^R)^T E,$$

wherein:

α and λ comprising hyperparameters that determine a structure of a machine learning network;

m represents a sample size of a mini batch Stochastic Gradient Descent (SGD) method;

X represents a $m \times k$ sample matrix;

each row of the matrix X represents a sample;

X_i represents the i^{th} row of the matrix X ;

$[j]$ represents the j^{th} element of vector X_i ;

X^L represents a first share of the sample data X that belongs to a first SCN of the plurality of secure computation nodes;

X^R represents the second share of the sample data X that belongs to a second SCN of the plurality of secure computation nodes;

Y represents a prediction value;

Y_i represents a label of the i^{th} sample of the mini batch SGD method;

E represents an error vector;

R , L , and T represent indexes of the shares of a respective SCN; and

Θ represents a parameter column vector, and the column vector Θ that is vertically dividable into Θ^L and Θ^R .

12. The non-transitory, computer-readable medium of claim 11, wherein calculating a share of A representing a column vector comprises:

encrypting original data provided by each SCN by using random numbers, and

exchanging the encrypted data between the plurality of secure computation

nodes.

13. The non-transitory, computer-readable medium of claim 12, wherein each of the random numbers is at least one of a number, a vector, or a matrix.

14. The non-transitory, computer-readable medium of claim 13, wherein the predetermined iteration condition is an occurrence of a difference between two consecutive iteration results that is less than a predetermined threshold.

15. A system, comprising:

one or more computers; and

one or more computer memory devices interoperably coupled with the one or more computers and having tangible, non-transitory, machine-readable media storing one or more instructions that, when executed by the one or more computers, perform one or more operations comprising:

dividing sample training data for a secure logistic regression model (SLRM) into a plurality of shares using secret sharing (SS) comprising hiding original data by encrypting the original data using random numbers generated by a plurality of secure computation nodes, such that the original data cannot be recovered by using a single share of the plurality of shares, wherein the sample training data is originating from the plurality of secure computation nodes configured to both produce and consume training data;

transmitting each share to one of the plurality of secure computation nodes;

generating updated parameters by iteratively updating current parameters associated with the SLRM using each share of the sample training data, wherein the iterative updating comprises:

for each SCN, calculating a value of A representing a column vector, wherein the calculating is performed based on the following equation:

$$A = X\Theta = X^L\Theta^L + X^R\Theta^R$$

wherein: $X^L\Theta^L$ and $X^R\Theta^R$ each represents a share of A for a SCN,

wherein calculating $X^L\theta^L$ and $X^R\theta^R$ comprises hiding original data provided from each SCN by using random numbers, and exchanging the hidden data between the SCNs;

determining that a predetermined iteration condition is satisfied; and

after iteratively updating the parameters associated with the SLRM, outputting a training result configured for use by each SCN of the plurality of secure computation nodes.

16. The system of claim 15, wherein an objective function of the SLRM is a logistic regression function that is optimized by using a mini batch Stochastic Gradient Descent (SGD) method, and wherein the logistic regression function is expressed as:

$$\theta[j] := \theta[j] - \frac{\alpha}{m} \sum_{i=1}^m (\text{sigmoid}(X_i^L \cdot \theta^L + X_i^R \cdot \theta^R) - Y_i) X_i[j] - \frac{\lambda}{m} \theta[j]$$

wherein:

α and λ comprising hyperparameters that determine a structure of a machine learning network;

m represents the sample size of the mini batch SGD;

X represents a $m \times k$ sample matrix;

each row of the matrix X represents a sample;

X_i represents an i^{th} row of the matrix X ;

$[j]$ represents a j^{th} element of vector X_i ;

X^L represents a share of the sample data X that belongs to a respective SCN;

X^R represents a share of the sample data X that belongs to the respective SCN; and

θ represents a parameter column vector that is vertically dividable into θ^L and θ^R .

17. The system of claim 15, wherein iteratively updating parameters associated with the SLRM is performed according to an event-driven model.

18. The system of claim 15, wherein iteratively updating parameters associated with the SLRM comprises:

determining a column vector of a prediction error based on the following equation:

$$E = g(A) - Y_i;$$

wherein:

g represents a fitting function of a sigmoid function, the fitting function comprising a polynomial fitting function; and

determining a updated column vector based on equation:

$$\theta := (1 - \frac{\lambda}{m})\theta - \frac{\alpha}{m} X^T E$$

wherein:

$$X^T E = (X^L)^T E || (X^R)^T E, \text{ wherein:}$$

α and λ comprising hyperparameters that determine a structure of a machine learning network;

m represents a sample size of a mini batch Stochastic Gradient Descent (SGD) method;

X represents a $m \times k$ sample matrix;

each row of the matrix X represents a sample;

X_i represents an i^{th} row of the matrix X ;

$[j]$ represents a j^{th} element of vector X_i ;

X^L represents a first share of the sample data X that belongs to a first SCN of the plurality of secure computation nodes;

X^R represents the second share of the sample data X that belongs to a second SCN of the plurality of secure computation nodes;

Y represents a prediction value;

Y_i represents a label of the i^{th} sample of the mini batch SGD method;

E represents an error vector;

R , L , and T represent indexes of the shares of a respective SCN; and

Θ represents a parameter column vector, and the column vector Θ that is vertically dividable into Θ^L and Θ^R .

19. The system of claim 18, wherein calculating a share of A representing a column vector comprises:

encrypting original data provided by each SCN by using random numbers, and

exchanging the encrypted data between the plurality of secure computation

nodes.

20. The system of claim 19, wherein each of the random numbers is at least one of a number, a vector, or a matrix.