

METHOD AND APPARATUS FOR PRIVATELY CALCULATING IV VALUES IN FEATURE ENGINEERING

FIELD

[0001] The present disclosure relates to the technical field of artificial intelligence, and in particular to a method and an apparatus for privately calculating IV values in feature engineering.

BACKGROUND

[0002] Information Value (IV) indicates contribution of a feature to target prediction, that is, indicates a prediction ability of a feature. Generally, a higher IV value indicates a feature having a stronger prediction ability and a higher information contribution degree. In machine learning algorithms, a higher IV value indicates that a feature containing more information and being more suitable for model training for the machine learning algorithms. However, with the increasing importance of data privacy and security protection, the method for calculating IV values based on data in plaintext does not meet the requirements for privacy protection.

[0003] According to the secure multi-party computation (MPC) technology, inputted data is shared secretly, each of multiple participants obtains a piece of shared data in ciphertext, and then an encryption computation is performed based on the shared data in ciphertext. Finally, a result in plaintext may be obtained based on results in ciphertext from the multiple participants. Each of the participants cannot infer data in plaintext inputted by other participants in the computation based on data in ciphertext.

[0004] Based on fully homomorphic encryption (FHE), the user may perform a calculation based on encrypted data without decrypting the data in advance. The calculation result is retained in ciphertext. The calculation result after being decrypted is the same as a result obtained by performing the calculation based on unencrypted data.

[0005] According to the conventional technology, although the privacy protection in calculating the IV values is achieved based on the MPC or FHE technology, it is required for a second participant obtaining feature values to be honest and credible in binning the features. If the second participant forges feature values in binning the features, the second participant may deduce a label value of a

sample of a first participant from a WOE calculation process with a high probability.

[0006] Specifically, it is assumed that a second participant wants to obtain a value a sample L_x (which is equal to 0 or 1, and it is assumed that a probability of a sample being 0 is equal to a probability of the sample being 1) of a first participant, the second participant constructs different feature bins in calculating WOE values of multiple features, and the only difference between the sample data included in two bins is that one bin includes L_x and the other bin does not include L_x . With the feature bins constructed in this way, the probability of inferring a label value of a sample of the first participant equal to 0 or 1 is greater than 50%.

[0007] Therefore, it is difficult to resist the dishonest attack from the second participant, that is, the feature value owner, in privately calculating the IV values according to the conventional privacy computing technology.

SUMMARY

[0008] Therefore, a method and an apparatus for privately calculating IV values in feature engineering are provided according to the present disclosure to solve the problem that the feature value owner forges the feature value data in binning the feature values for privately computing the IV values according to the conventional technology.

[0009] To achieve the above purpose, the following technical solutions are provided according to the present disclosure.

[0010] In a first aspect, a method for privately calculating IV values in feature engineering is provided according to the present disclosure. In the method, a first participant interacts with a second participant in an MPC environment to calculate the IV values, the first participant obtains label values of samples and the second participant obtains feature values of the samples, and the label values of the samples obtained by the first participant is confidential to the second participant and the feature values of the samples obtained by the second participant is confidential to the first participant. The method is applied to the first participant. The method includes: receiving feature value binning information from the second participant, where the feature value binning information is a random number assigned to feature values binned in a same bin after the second participant bins the feature values; calculating IV values for all bins based on the label values of the samples, and determining whether malicious

grouping is performed based on the feature value binning information from the second participant in calculating the IV values; in a case that malicious grouping is performed, stopping calculating the IV values; and in a case that malicious grouping is not performed, transmitting calculated IV values to the second participant.

[0011] In an embodiment, the second participant bins the feature values with an equidistant binning algorithm.

[0012] In an embodiment, the second participant in binning the feature values equidistantly bins the feature values evenly.

[0013] In an embodiment, when the second participant bins the feature values, it is allowed to disclose to the first participant that certain samples belong to a same bin, and it is not allowed to disclose to the first participant the number of the bin.

[0014] In an embodiment, the malicious grouping is performed by configuring two groups to have a few sample differences.

[0015] In a second aspect, a method for privately calculating IV values in feature engineering is provided according to the present disclosure. In the method, a first participant and a second participant cooperate to calculate the IV values in an MPC environment, the first participant obtains label values of samples and the second participant obtains feature values of the samples, and the label values of the samples obtained by the first participant is confidential to the second participant and the feature values of the samples obtained by the second participant is confidential to the first participant. The method includes: binning, by the second participant, the feature values; for each of bins, assigning, by the second participant, a random number to the bin, and assigning, by the second participant, the random number to feature values in the bin; transmitting, by the second participant, random numbers corresponding to all the feature values to the first participant; calculating, by the first participant, IV values of features based on the label values of the samples and received feature value binning information; and determining, by the first participant, whether a dishonest attack is performed based on the feature value binning information from the second participant, and in a case that the dishonest attack is not performed, transmitting calculated IV values to the second participant.

[0016] In a third aspect, an apparatus for privately calculating IV values in feature engineering is provided according to the present disclosure. A first participant interacts with a second participant in

an MPC environment to calculate the IV values, the first participant obtains label values of samples and the second participant obtains feature values of the samples, and the label values of the samples obtained by the first participant is confidential to the second participant and the feature values of the samples obtained by the second participant is confidential to the first participant. The apparatus is configured to perform steps performed by the first participant. The apparatus includes the following program modules: a reception module, an IV value calculation module, and a malicious grouping determination module.

[0017] The reception module is configured to receive feature value binning information from the second participant. The feature value binning information is a random number assigned to feature values binned in a same bin after the second participant bins the feature values.

[0018] The IV value calculation module is configured to calculate IV values for all bins based on the label values of the samples.

[0019] The malicious grouping determination module is configured to: determine whether malicious grouping is performed based on the feature value binning information from the second participant in calculating the IV values; in a case that malicious grouping is performed, stop calculating the IV values; and in a case that malicious grouping is not performed, transmit calculated IV values to the second participant.

[0020] In a fourth aspect, a computer device is provided according to the present disclosure. The computer device includes a memory and a processor. The memory stores a computer program. The processor is configured, when executing the computer program, to perform the method for privately calculating IV values in feature engineering.

[0021] In a fifth aspect, a computer readable storage medium is provided according to the present disclosure. The computer readable storage medium stores a computer program. The computer program, when executed by a processor, causes the processor to perform the method for privately calculating IV values in feature engineering.

[0022] Compared with the conventional technology, at least the following advantageous effects can be achieved with the present disclosure.

[0023] A method and an apparatus for privately calculating IV values in feature engineering are provided according to the present disclosure. The method includes: receiving feature value binning

information from the second participant, where the feature value binning information is a random number assigned to feature values binned in a same bin after the second participant bins the feature values; calculating IV values for all bins based on the label values of the samples, and determining whether malicious grouping is performed based on the feature value binning information from the second participant in calculating the IV values; in a case that malicious grouping is performed, stopping calculating the IV values; and in a case that malicious grouping is not performed, transmitting calculated IV values to the second participant. With the method for privately calculating IV values in feature engineering according to the present disclosure, the first participant can determine whether a feature value grouping result from the second participant is malicious, thereby protecting the privacy of data of participants.

BRIEF DESCRIPTION OF THE DRAWINGS

[0024] In order to intuitively illustrate the conventional technology and the present disclosure, several exemplary accompanying drawings are provided below. It should be understood that the specific shapes and constructions shown in the accompanying drawings are not limitations for the realization of the present disclosure. For example, those skilled in the art can easily make conventional adjustments or further optimizations to the addition/subtraction/attribution division, specific shapes, positional relationships, connection manners, dimensional proportional relationships and the like of units (components) based on the technical concept and the exemplary accompanying drawings of the present disclosure.

[0025] Figure 1 is a flowchart of a method for privately calculating IV values in feature engineering (an execution process performed by a first participant) according to an embodiment of the present disclosure; and

[0026] Figure 2 is a flowchart of a method for privately calculating IV values in feature engineering (an execution process performed by two participants) according to an embodiment of the present disclosure.

DETAILED DESCRIPTION

[0027] Hereinafter, the present disclosure is further described in detail with reference to specific

embodiments and in conjunction with the accompanying drawings.

[0028] In the description of the present disclosure: unless otherwise stated, the term "multiple" means two or more. The terms "first", "second", "third" and the like in the present disclosure are intended to distinguish the referred objects and have no particular meaning in terms of technical connotation (for example, they should not be understood as an emphasis on importance, order, or the like). The expressions "including", "containing", "having" or the like also imply "is not limited to" (units, elements, materials, steps, or the like).

[0029] The terms "top", "bottom", "left", "right", "middle" and the like in the present disclosure are generally intended to be understood visually with reference to the accompanying drawings, and are not absolute limitations on position relationships of actual products. Without departing from the technical concept disclosed in the present disclosure, changes in relative position relationships should be considered to be within the scope of the present disclosure.

[0030] The method for calculating IV values in plaintext in feature engineering is conventional technology, and is described as follows.

[0031] The initial conditions are defined as follows. It is assumed that there are m samples and n features, and a label value of a sample is represented as $L_i \in \{0, 1\}$, where for a positive sample, $L_i=1$, and for a negative sample, $L_i=0$. The number of all positive samples is represented as G_{total} , and the number of all negative samples is represented as B_{total} . For each of features, the following calculation process including steps S101 to S106 are performed.

[0032] In step S101, m sample values of the feature are binned. For example, the m sample values may be equidistantly binned, or may be evenly binned based on the feature values. It is assumed that the number of bins is N , then there are N groups, each of the groups is represented as Grp_i , and each of the groups includes m_i samples where $m_i=[m/N]$.

[0033] In step S102, the number of all positive samples included in a group Grp_i (where $i \in [1, N]$) is represented as G_i , the number of all negative samples in the group Grp_i is represented as B_i , then the following equations are obtained:

$$G_{total} = \sum_{i=1}^N G_i, \quad B_{total} = \sum_{i=1}^N B_i$$

[0034] In step S103, a WOE value is calculated for each of the groups by using the following

equation:

$$WOE_i = \log\left(\frac{G_i}{G_{total}} / \frac{B_i}{B_{total}}\right)$$

[0035] In step S104, a total WOE value is calculated for the feature by using the following equation:

$$WOE = \sum_{i=1}^N \log\left(\frac{G_i}{G_{total}} / \frac{B_i}{B_{total}}\right)$$

[0036] In step S105, an IV value is calculated for each of the groups by using the following equation:

$$IV_i = \left(\frac{G_i}{G_{total}} - \frac{B_i}{B_{total}}\right) \times WOE_i = \left(\frac{G_i}{G_{total}} - \frac{B_i}{B_{total}}\right) \times \log\left(\frac{G_i}{G_{total}} / \frac{B_i}{B_{total}}\right)$$

[0037] In step S106, an IV value of a feature is calculated by using the following equation:

$$IV = \sum_{i=1}^N \left(\left(\frac{G_i}{G_{total}} - \frac{B_i}{B_{total}} \right) \log\left(\frac{G_i}{G_{total}} / \frac{B_i}{B_{total}}\right) \right)$$

[0038] Specifically, in calculating IV values in feature engineering by using a privacy computing technology such as MPC or FHE, the general participants and security assumptions are defined as follows.

[0039] The participants include a first participant and a second participant. It is assumed that the first participant obtains label values of m samples where each of the label values of the samples is represented as $L_i \in \{0, 1\}$, and the second participant obtains n feature values of the samples. According to the privacy computing technology, the label values of the samples obtained by the first participant is confidential to the second participant, and the feature values of the samples obtained by the second participant is confidential to the first participant.

[0040] In calculating the WOE value after features are grouped, the first participant inputs the label values and the second participant inputs the feature values, and the first participant and the second

participant perform encryption calculation by using MPC technology. The first participant and the second participant may only obtain the WOE values, and the data inputted by one of the first participant and the second participant cannot be obtained by the other one of the first participant and the second participant.

[0041] Therefore, a method for privately calculating IV values in feature engineering is provided according to the present application. The method is applied in an MPC environment. The first participant and the second participant cooperate to calculate the IV values. The first participant obtains label values of samples, and the second participant obtains feature values of the samples. The label values of the samples obtained by the first participant is confidential to the second participant and the feature values of the samples obtained by the second participant is confidential to the first participant.

[0042] Referring to Figure 1, the method includes the following steps S1 to S4.

[0043] In step S1, feature value binning information is received from the second participant. The feature value binning information is a random number assigned to feature values binned in a same bin after the second participant bins the feature values

[0044] Specifically, the second participant in binning the feature values equidistantly bins the feature values evenly. When the second participant bins the feature values, it is allowed to disclose to the first participant that certain samples belong to a same bin, and it is not allowed to disclose to the first participant the number of the bin.

[0045] In step S2, IV values for all bins are calculated based on the label values of the samples, and it is determined whether malicious grouping is performed based on the feature value binning information from the second participant in calculating the IV values.

[0046] In step S3, the calculation of the IV values is stopped in a case that malicious grouping is performed.

[0047] In step S4, calculated IV values are transmitted to the second participant in a case that malicious grouping is not performed.

[0048] Specifically, the malicious grouping may be performed by configuring two groups to have a few sample differences.

[0049] An example of the interaction between the two participants is provided below.

[0050] The first participant and the second participant synchronously perform calculation under the

condition that, the first participant and the second participant jointly calculate IV values, the first participant obtains label values of m samples, and the second participant obtains all feature values of the m samples.

[0051] The security requirement includes that the first participant cannot obtain a feature value of a sample from the second participant, and the second participant cannot obtain a label value of a sample from the first participant.

[0052] Referring to Figure 2, an IV value of a feature is calculated by performing the following steps S1 to S4.

[0053] In step S1, the second participant bins the feature values. For each of bins, the second participant assigns a random number to the bin and assigns the random number to feature values in the bin.

[0054] Specifically, the second participant bins the m features values equidistantly. It is assumed that the number of bins is N , there are N groups, each of the groups is represented as Grp_i , and the number of samples in each of the groups is represented as m_i where $m_i = \lceil m/N \rceil$. The second participant generates N random numbers, and each of the random numbers is represented as r_i , $i \in [1, N]$. Each of the groups G_i is assigned with a random number r_i .

[0055] In step S2, the second participant transmits random numbers corresponding to all the feature values to the first participant.

[0056] Specifically, for each of the group G_i , the second participant assigns a same random number r_i to all the feature values in the group G_i and transmits the random number r_i corresponding to the feature values to the first participant.

[0057] In step S3, the first participant calculates the IV values of features based on the label values of the samples and received feature value binning information.

[0058] Specifically, after receiving the random number r_i of each of the feature values from the second participant, the first participant calculates a WOE value and an IV value for the feature values corresponding to the same r_i based on the label values of the samples. The detail calculation process includes the following steps S31 to S34.

[0059] It is assumed that the number of all positive samples included in a group G_i is represented as G_i and the number of all negative samples in the group G_i is represented as B_i , then the following

equations are obtained:

$$G_{\text{total}} = \sum_{i=1}^N G_i, \quad B_{\text{total}} = \sum_{i=1}^N B_i$$

[0060] In step S31, a WOE value is calculated for a group by using the following equation:

$$\text{WOE}_i = \log \left(\frac{G_i}{G_{\text{total}}} / \frac{B_i}{B_{\text{total}}} \right)$$

[0061] In step S32, a total WOE value is calculated by using the following equation:

$$\text{WOE} = \sum_{i=1}^N \log \left(\frac{G_i}{G_{\text{total}}} / \frac{B_i}{B_{\text{total}}} \right)$$

[0062] In step S33, an IV value is calculated for each of the groups by using the following equation:

$$\text{IV}_i = \left(\frac{G_i}{G_{\text{total}}} - \frac{B_i}{B_{\text{total}}} \right) \times \text{WOE}_i = \left(\frac{G_i}{G_{\text{total}}} - \frac{B_i}{B_{\text{total}}} \right) \times \log \left(\frac{G_i}{G_{\text{total}}} / \frac{B_i}{B_{\text{total}}} \right)$$

[0063] In step S34, an IV value for a feature is calculated by using the following equation:

$$\text{IV} = \sum_{i=1}^N \left(\left(\frac{G_i}{G_{\text{total}}} - \frac{B_i}{B_{\text{total}}} \right) \log \left(\frac{G_i}{G_{\text{total}}} / \frac{B_i}{B_{\text{total}}} \right) \right)$$

[0064] In step S4, the first participant determines whether a dishonest attack is performed based on the feature value binning information from the second participant, and in a case that the dishonest attack is not performed, the first participant transmits calculated IV values to the second participant.

[0065] Specifically, after receiving a random number r_i of each of the feature values from the second participant, the first participant determines whether the second participant maliciously constructs feature value bins. In a case that the second participant maliciously constructs feature value bins, the first participant stops calculating the IV values. In a case that the second participant does not maliciously construct feature value bins, the first participant transmits the calculated IV values to the second participant.

[0066] According to the present disclosure, privacy computing technology is adopted to jointly calculate IV values by two participants. The label value owner may detect and resist dishonest attacks

from the feature value owner, meeting the traditional data privacy protection requirements. That is, the label value data provider cannot obtain the feature data from the feature value data provider. In addition, the feature value data provider cannot obtain the label value data from the label value data provider, preventing dishonest attacks from the feature value owner. In a case that the feature value data provider constructs malicious feature groups to obtain a label value from the label value owner, the label value owner can detect that the feature value data provider constructs malicious feature groups and stops the joint computation, thereby protecting the privacy of data of the participants.

[0067] An apparatus for privately calculating IV values in feature engineering is further provided according to the present disclosure. The apparatus is applied in an MPC environment in which a first participant and a second participant jointly calculate the IV values, the first participant obtains label values of samples and the second participant obtains feature values of the samples, and the label values of the samples obtained by the first participant is confidential to the second participant and the feature values of the samples obtained by the second participant is confidential to the first participant.

[0068] The apparatus includes a reception module, an IV value calculation module and a malicious grouping determination module.

[0069] The reception module is configured to receive feature value binning information from the second participant. The feature value binning information is a random number assigned to feature values binned in a same bin after the second participant bins the feature values.

[0070] The IV value calculation module is configured to calculate IV values for all bins based on the label values of the samples.

[0071] The malicious grouping determination module is configured to: determine whether malicious grouping is performed based on the feature value binning information from the second participant in calculating the IV values; in a case that malicious grouping is performed, stop calculating the IV values; and in a case that malicious grouping is not performed, transmit calculated IV values to the second participant.

[0072] The specific limitations of the apparatus for privately calculating IV values in feature engineering may refer to the limitations for the method for privately calculating IV values in feature engineering, and are not repeated herein.

[0073] A computer device is further provided according to the present disclosure. The computer

device includes a memory and a processor. The memory stores a computer program thereon. The processor is configured, when executing the computer program, to perform the method for privately calculating IV values in feature engineering.

[0074] A computer readable storage medium is further provided according to the present disclosure. The computer readable storage medium stores a computer program. The computer program, when executed by a processor, causes the processor to perform the method for privately calculating IV values in feature engineering.

[0075] The technical features in the above embodiments may be combined arbitrarily (as long as the combination of these technical features is not contradictory). To make the description concise, not all possible combinations of the technical features in the above embodiments are described. These embodiments that are not described should be considered within the scope of the present specification.

[0076] The present disclosure has been described in detail through general descriptions and specific embodiments. It should be understood that conventional adaptations or further innovations may be made to these specific embodiments based on the technical concept of the present disclosure. However, the technical solutions obtained based on the conventional adaptations or further innovations without departing from the technical concept of the present disclosure still fall within the protection scope of the claims in the present disclosure.

CLAIMS

1. A method for privately calculating IV values in feature engineering, wherein a first participant interacts with a second participant in an MPC environment to calculate the IV values, the first participant obtains label values of samples and the second participant obtains feature values of the samples, and the label values of the samples obtained by the first participant is confidential to the second participant and the feature values of the samples obtained by the second participant is confidential to the first participant, wherein

the method is applied to the first participant, and comprises:

receiving feature value binning information from the second participant, wherein the feature value binning information is a random number assigned to feature values binned in a same bin after the second participant bins the feature values;

calculating IV values for all bins based on the label values of the samples, and determining whether malicious grouping is performed based on the feature value binning information from the second participant in calculating the IV values;

in a case that malicious grouping is performed, stopping calculating the IV values; and

in a case that malicious grouping is not performed, transmitting calculated IV values to the second participant.

2. The method for privately calculating IV values in feature engineering according to claim 1, wherein the second participant bins the feature values with an equidistant binning algorithm.

3. The method for privately calculating IV values in feature engineering according to claim 2, wherein the second participant, in binning the feature values equidistantly, evenly bins the feature values.

4. The method for privately calculating IV values in feature engineering according to claim 1, wherein when the second participant bins the feature values, it is allowed to disclose to the first participant that some samples belong to a same bin, and it is not allowed to disclose to the first participant the number of the bin.

5. The method for privately calculating IV values in feature engineering according to claim 1, wherein the malicious grouping is performed by configuring two groups to have a few sample

differences.

6. A method for privately calculating IV values in feature engineering, wherein a first participant and a second participant jointly calculate the IV values in an MPC environment, the first participant obtains label values of samples and the second participant obtains feature values of the samples, and the label values of the samples obtained by the first participant is confidential to the second participant and the feature values of the samples obtained by the second participant is confidential to the first participant, wherein

the method comprises:

binning, by the second participant, the feature values;

for each of bins, assigning, by the second participant, a random number to the bin, and assigning, by the second participant, the random number to feature values in the bin;

transmitting, by the second participant, random numbers corresponding to all the feature values to the first participant;

calculating, by the first participant, IV values of features based on the label values of the samples and received feature value binning information; and

determining, by the first participant, whether a dishonest attack is performed based on the feature value binning information from the second participant, and in a case that the dishonest attack is not performed, transmitting calculated IV values to the second participant.

7. An apparatus for privately calculating IV values in feature engineering, wherein a first participant interacts with a second participant in an MPC environment to calculate the IV values, the first participant obtains label values of samples and the second participant obtains feature values of the samples, and the label values of the samples obtained by the first participant is confidential to the second participant and the feature values of the samples obtained by the second participant is confidential to the first participant, wherein

the apparatus is configured to perform steps performed by the first participant, and comprises the following program modules:

a reception module, configured to receive feature value binning information from the second participant, wherein the feature value binning information is a random number assigned to feature values binned in a same bin after the second participant bins the feature values;

an IV value calculation module, configured to calculate IV values for all bins based on the label values of the samples; and

a malicious grouping determination module, configured to:

determine whether malicious grouping is performed based on the feature value binning information from the second participant in calculating the IV values;

in a case that malicious grouping is performed, stop calculating the IV values; and

in a case that malicious grouping is not performed, transmit calculated IV values to the second participant.

8. A computer device, comprising:

a memory, storing a computer program; and

a processor; wherein

the processor is configured, when executing the computer program, to perform the method according to any one of claims 1 to 5.

9. A computer readable storage medium, storing a computer program, wherein the computer program, when executed by a processor, causes the processor to perform the method according to any one of claims 1 to 5.