US 20250265316A1

(19) **United States**

(12) **Patent Application Publication** (10) **Pub. No.: US 2025/0265316 A1**

MIURA et al. (43) **Pub. Date: Aug. 21, 2025**

(54) **INFORMATION PROCESSING DEVICE AND INFORMATION PROCESSING METHOD**

(71) Applicant: **TOYOTA JIDOSHA KABUSHIKI KAISHA**, Toyota-shi (JP)

(72) Inventors: **Naritomo MIURA**, Miyoshi-shi (JP); **Shinya Miyasaka**, Okazaki-shi (JP); **Naoki Ishihara**, Nisshin-shi (JP)

(73) Assignee: **TOYOTA JIDOSHA KABUSHIKI KAISHA**, Toyota-shi (JP)

(21) Appl. No.: **18/955,108**

(22) Filed: **Nov. 21, 2024**

(30) **Foreign Application Priority Data**

Feb. 19, 2024 (JP) 2024-022791

Publication Classification

(51) **Int. Cl.**
G06F 21/12 (2013.01)

(52) **U.S. Cl.**
CPC ***G06F 21/12*** (2013.01)

(57) **ABSTRACT**

The disclosure relates to an information processing device. The information processing device includes: an acquisition unit that acquires information on artificial data generated by a generative AI constructed by machine learning using user data including information capable of specifying an individual; and a generation unit that generates a transaction including information on artificial data.

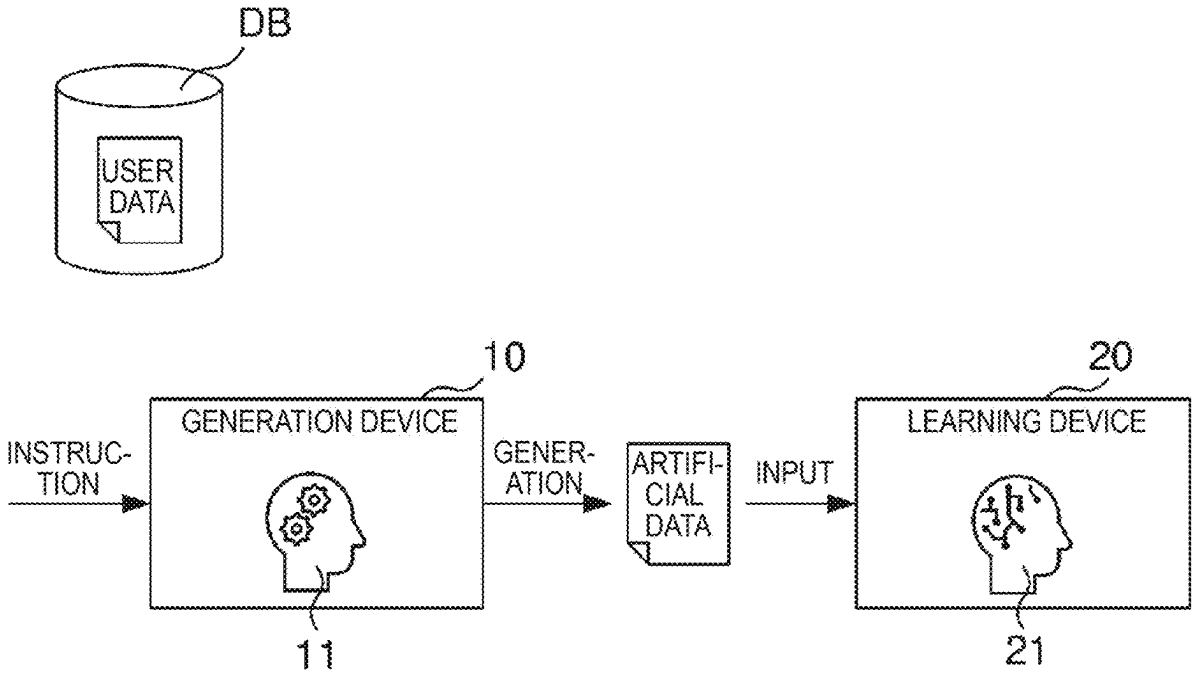


FIG. 1

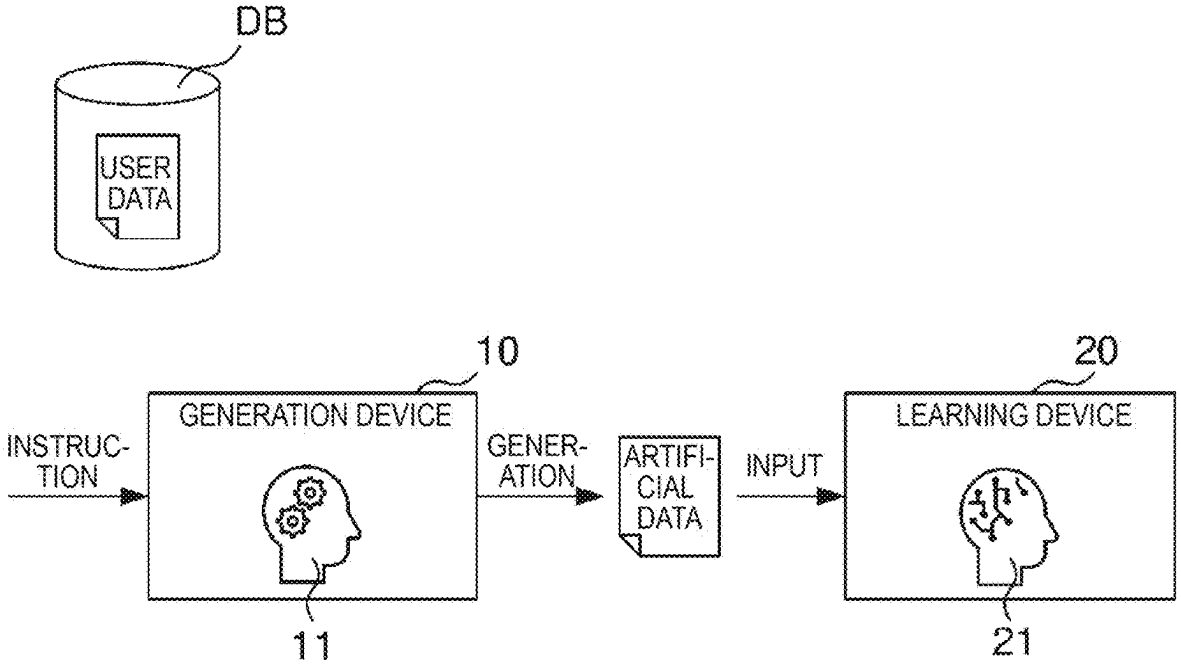

DB
USER DATA
10
GENERATION DEVICE
INSTRUC-TION
GENER-ATION
ARTIFI-CIAL DATA
INPUT
20
LEARNING DEVICE
11
21

FIG. 2

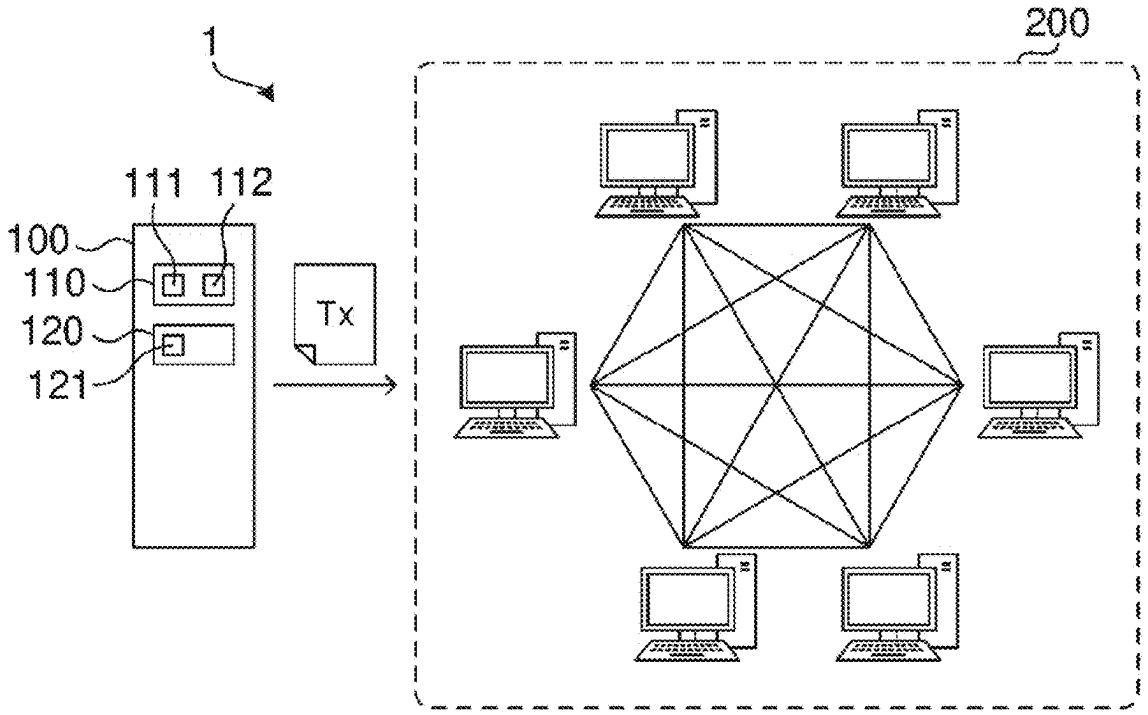
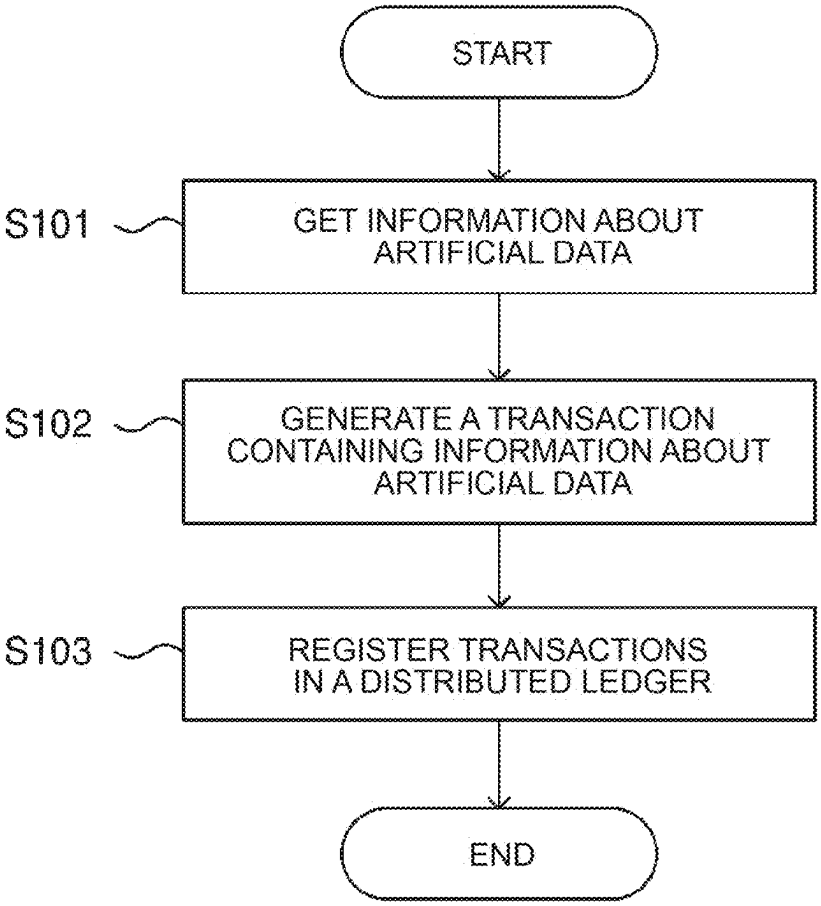

1
200
111
112
100
110
120
121
Tx

FIG. 3


START
S101
GET INFORMATION ABOUT ARTIFICIAL DATA
S102
GENERATE A TRANSACTION CONTAINING INFORMATION ABOUT ARTIFICIAL DATA
S103
REGISTER TRANSACTIONS IN A DISTRIBUTED LEDGER
END

INFORMATION PROCESSING DEVICE AND INFORMATION PROCESSING METHOD

CROSS-REFERENCE TO RELATED APPLICATION

[0001] This application claims priority to Japanese Patent Application No. 2024-022791 filed on Feb. 19, 2024, incorporated herein by reference in its entirety.

BACKGROUND

1. Technical Field

[0002] The present disclosure relates to the technical field of information processing devices and information processing methods.

2. Description of Related Art

[0003] There is proposed a device that divides data into sensitive data and non-sensitive data and that provides the non-sensitive data to a distributed ledger, for example (see Japanese Unexamined Patent Application Publication (Translation of PCT Application) No. 2022-511393 (JP 2022-511393 A)).

SUMMARY

[0004] The behavior of a learned model constructed through machine learning is occasionally verified. This verification is often performed after a certain period of time has elapsed since the learned model was constructed. Although learning data used for the machine learning for constructing the learned model are used for the verification, there is a possibility that the reliability of the learning data is not guaranteed. JP 2022-511393 A does not consider the verification of the behavior of the learned model.

[0005] The present disclosure has been made in view of the above circumstances, and an object of the present disclosure is to provide an information processing device and an information processing method that can ensure the reliability of learning data.

[0006] An aspect of the present disclosure provides an information processing device including: an acquisition unit that acquires information about artificial data generated by a generative artificial intelligence (AI) built through machine learning using user data including information that enables personal identification, the artificial data not including information that enables personal identification; and

[0007] a generation unit that generates a transaction including information about the artificial data.

[0008] An aspect of the present disclosure provides an information processing method including: acquiring information about artificial data generated by a generative artificial intelligence (AI) built through machine learning using user data including information that enables personal identification, the artificial data not including information that enables personal identification;

[0009] generating a transaction including information about the artificial data; and

[0010] storing the transaction in a distributed ledger.

BRIEF DESCRIPTION OF THE DRAWINGS

[0011] Features, advantages, and technical and industrial significance of exemplary embodiments of the disclosure will be described below with reference to the accompanying drawings, in which like signs denote like elements, and wherein:

[0012] FIG. **1** is a conceptual diagram illustrating an example of machine learning;

[0013] FIG. **2** is a block diagram illustrating a configuration of an information processing system according to an embodiment; and

[0014] FIG. **3** is a flowchart illustrating an operation of the information processing system according to the embodiment.

DETAILED DESCRIPTION OF EMBODIMENTS

[0015] Embodiments of an information processing device and an information processing method will be described with reference to FIGS. **1** to **3**.

[0016] First, an example of machine learning will be described with reference to FIG. **1**. In FIG. **1**, user data is registered in the database DB. Here, at least a part of the user data may be data including information capable of specifying an individual. The user data may be, for example, image data including a face of the user. That is, the user data may be image data related to an image in which the face of the user is captured. Such user data may be generated, for example, by capturing an image of a person riding on the vehicle by a camera (for example, a driver monitor camera) that captures an image of the inside of the vehicle.

[0017] The generation device **10** includes a generative AI (Artificial Intelligence) **11**. The generative AI **11** is a generative AI constructed by performing training using user data (typically a plurality of user data) registered in the database DB. It is to be noted that various aspects of the present disclosure can be applied to methods of constructing a generative AI **11**. Therefore, detailed explanation of how to construct the generative AI **11** will be omitted. Note that the generative AI **11** may be constructed by fine tuning in which a pre-learned model (for example, a base model) is re-learned using user data.

[0018] The generation device **10** may receive an instruction from an operator of the generation device **10**. The instruction by the operator may be represented by textual information. The generation device **10** may enter an instruction from the operator into the generative AI **11**. generative AI **11** instructed by the operator is inputted may generate an artificial datum according to the instruction. That is, the generation device **10** may generate artificial data using the generative AI **11**.

[0019] For example, when the user data is image data including the face of the user, the generative AI **11** learned by using the user data may be capable of generating new image data including the face as the artificial data. For example, when the instruction of the operator is "a face of a woman in her 70s", the generative AI **11** may generate image data including a face of an imaginary woman in her 70s as the artificial data. For example, when the instruction of the operator is "a face of a man in his/her twenties", the generative AI **11** may generate image data including a face of an imaginary man in his/her twenties as the artificial data. Note that the generative AI may generate one artificial data or a plurality of artificial data for one instruction of the operator.

[0020] For example, the image data including the face of the user corresponds to personal information. Therefore, it can be said that the image data including the face of the user

as the user data includes information capable of specifying the individual. On the other hand, the image data generated by the generative AI **11** and including the face of the fictional person does not correspond to the information that can identify the individual. Therefore, it can be said that the artificial data is data that does not include information capable of specifying an individual. As described above, by generating artificial data using the generative AI **11**, it is possible to generate a large amount of data that does not include information capable of identifying individuals.

[0021] The learning device **20** includes an arithmetic model **21**. The arithmetic model **21** is a model before machine learning is performed (for example, a model in which weighting is not optimized). The learning device **20** may learn the arithmetic model **21** using artificial data (typically, a plurality of artificial data) generated by the generation device **10** (specifically, the generative AI **11**). Note that various existing aspects can be applied to the learning method of the arithmetic model **21**. Therefore, detailed description of the learning method of the arithmetic model **21** will be omitted.

[0022] Next, the information processing system **1** according to the embodiment will be described with reference to FIG. **2** and FIG. **3**. In FIG. **2**, the information processing system **1** includes an information processing device **100** and a distributed network **200** including a plurality of nodes. The information processing device **100** may be, for example, a server apparatus such as an application server or a terminal apparatus such as a personal computer.

[0023] The information processing system **1** registers information on artificial data used for machine learning of the arithmetic model **21** in a distributed ledger (for example, a blockchain) realized by the distributed network **200**. For example, the information processing system **1** may function as a database related to artificial data.

[0024] The information processing device **100** may include an arithmetic device **110** and a storage device **120**. The arithmetic device **110** may include, for example, at least one of CPU (Central Processing Unit) and GPU (Graphics Processing Unit). The storage device **120** may include, for example, at least one of RAM (Random Access Memory) and ROM (Read Only Memory). The storage device **120** may include, for example, at least one of a hard disk device, a magneto-optical disk device, an SSD (Solid State Drive), and an optical disk array. That is, it can be said that the information processing device **100** includes at least one processor and at least one memory.

[0025] The storage device **120** may store a computer program **121**. The arithmetic device **110** may execute processing to be performed by the information processing device **100** together with the storage device **120** in which the computer program **121** is stored (in other words, together with the storage device **120** and the computer program **121** stored in the storage device **120**). For example, a logical functional block for executing a process to be performed by the information processing device **100** may be realized in the arithmetic device **110** by the arithmetic device **110** executing the computer program **121**. For example, the arithmetic device **110** may include an acquisition unit **111** and a generation unit **112** as functional blocks.

[0026] The acquisition unit **111** of the arithmetic device **110** acquires information related to artificial data from the generation device **10** (see FIG. **1**). The information on the artificial data may be, for example, artificial data itself, information for identifying the artificial data, information for specifying the artificial data, or information indicating the location of the artificial data.

[0027] An example of information for identifying artificial data is a hash value generated from artificial data. An example of information for specifying artificial data is a file name related to artificial data. Examples of the information indicating the location of the artificial data include information (for example, Uniform Resource Locator: URL) indicating the location where the artificial data is recorded.

[0028] The generation unit **112** of the arithmetic device **110** generates a transaction including information related to artificial data. The arithmetic device **110** may transmit the generated transaction to the distributed network **200**. At least one node constituting the distributed network **200** may verify a transaction transmitted from the information processing device **100**, and then register the transaction in the distributed ledger.

[0029] When the information related to the artificial data is the artificial data itself, the arithmetic device **110** may generate a transaction including the artificial data. In this case, the artificial data is registered in the distributed ledger. When the information on the artificial data is not the artificial data itself (for example, when the information on the artificial data is a hash value generated from the artificial data), the artificial data may be stored in the storage device **120** of the information processing device **100**, for example. Alternatively, the information processing system **1** may include a device that stores artificial data different from the information processing device **100**.

[0030] Next, the operation of the information processing system **1** will be described with reference to the flowchart of FIG. **3**. In FIG. **3**, the acquisition unit **111** of the arithmetic device **110** of the information processing device **100** acquires information related to artificial data from the generation device **10** (S**101**). Next, the generation unit **112** of the arithmetic device **110** generates a transaction including information related to artificial data (S**102**). The arithmetic device **110** may then transmit the transaction to the distributed network **200**. At least one node of the distributed network **200** may register the transaction into a distributed ledger (S**103**).

Technical Effect

[0031] By performing machine learning of the arithmetic model (for example, the arithmetic model **21**), the behavior of the learned model may be verified after the learned model is constructed. For verification, learning data used for machine learning of the arithmetic model is used.

[0032] By the way, a service provider may collect user data after obtaining the user's consent. The operator may perform machine learning of the arithmetic model by using the collected user data as learning data. On the other hand, the user can request the operator to delete the user data collected by the operator (in other words, provided by the user). When at least a part of the user data as the learning data is deleted in accordance with the user data deletion request, it may be difficult to verify the behavior of the learned model.

[0033] On the other hand, in the present embodiment, the machine learning of the arithmetic model **21** is performed using the artificial data generated by the generation device **10** (specifically, the generative AI **11**). That is, the user data registered in the database DB is not used for the machine

learning of the arithmetic model **21**. Therefore, artificial data is used to verify the behavior of the learned model constructed by performing the machine learning of the arithmetic model **21**. Therefore, even if the user data registered in the database DB is deleted due to the user data deletion request, the behavior of the learned model using the artificial data is not verified.

[0034] In the present embodiment, in particular, information on artificial data used for machine learning of the arithmetic model **21** is registered in the distributed ledger. It is extremely difficult to falsify the information on the artificial data registered in the distributed ledger. Therefore, by referring to the information on the artificial data registered in the distributed ledger, it is possible to detect the altered artificial data even if the artificial data is altered. For example, if the artificial data itself is registered in the distributed ledger as the information on the artificial data, it is possible to suppress the artificial data being altered. That is, according to the present embodiment, it is possible to suppress a decrease in the reliability of the artificial data.

[0035] As described above, according to the present embodiment, it is possible to protect the right to request the user to delete the data, and to ensure the reliability of the artificial data used for verifying the behavior of the learned model. Since the reliability of the artificial data is ensured, it is expected that the learned model is appropriately verified.

[0036] Various modes of the disclosure derived from the embodiment described above will be described below.

[0037] An information processing device according to an aspect of the present disclosure includes: an acquisition unit that acquires information related to artificial data generated by a generative AI constructed by machine learning using user data including information capable of specifying an individual; and a generation unit that generates a transaction including information related to the artificial data. In the above-described embodiment, the acquisition unit **111** corresponds to an example of an acquisition unit, and the generation unit **112** corresponds to an example of a generation unit.

[0038] Here, the transaction may include a hash value generated from the artificial data as information about the artificial data. Alternatively, the transaction may include the artificial data as information about the artificial data. The artificial data may be data used for machine-learning of a computational model that differs from the generative AI.

[0039] An information processing method according to an aspect of the present disclosure includes: an acquisition step of acquiring information related to artificial data generated by a generative AI constructed by machine learning using user data including information capable of specifying an individual; a generation step of generating a transaction including information related to the artificial data; and a storage step of storing the transaction in a distributed ledger.

[0040] The present disclosure is not limited to the above-described embodiments, and can be modified as appropriate within the scope and spirit of the disclosure that can be read from the claims and the entire specification. An information processing device and an information processing method accompanied by such a change are also included in the technical scope of the present disclosure.

What is claimed is:

1. An information processing device comprising:

an acquisition unit that acquires information about artificial data generated by a generative artificial intelligence (AI) built through machine learning using user data including information that enables personal identification, the artificial data not including information that enables personal identification; and

a generation unit that generates a transaction including information about the artificial data.

2. The information processing device according to claim **1**, wherein the transaction includes a hash value generated from the artificial data as the information about the artificial data.

3. The information processing device according to claim **1**, wherein the transaction includes the artificial data as the information about the artificial data.

4. The information processing device according to claim **1**, wherein the artificial data are data to be used for machine learning of a computation model that is different from the generative AI.

5. An information processing method comprising:

acquiring information about artificial data generated by a generative artificial intelligence (AI) built through machine learning using user data including information that enables personal identification, the artificial data not including information that enables personal identification;

generating a transaction including information about the artificial data; and

storing the transaction in a distributed ledger.

* * * * *