

CONTROL METHOD AND APPARATUS FOR INTELLIGENT VENDING CABINET, ELECTRONIC DEVICE, AND STORAGE MEDIUM

CROSS-REFERENCE TO RELATED APPLICATION

[0001] The present application claims priority to Chinese patent application No. 202110455765.4 filed on April 26, 2021, entitled “Control Method and Apparatus for Intelligent Vending cabinet, Electronic Device, and Storage Medium”, which is hereby incorporated by reference in its entirety.

FIELD

[0002] The present application relates to the field of equipment control, in particular to a control method and device for an intelligent vending cabinet, an electronic device, and a storage medium.

BACKGROUND

[0003] Various goods are placed in an intelligent vending cabinet, and a user may request to open a door by scanning a quick response (QR) code, and then take the goods. The intelligent vending cabinet includes two control systems of which one control system, as an upper computer, interacts with a cloud terminal, and the other control system, as a lower computer, interacts with an electronically controlled lock.

[0004] During the use of the intelligent vending cabinet, the electronically controlled lock is controlled by the lower computer that sends an unlocking signal (level signal), and the electronically controlled lock itself is unable to verify the legitimacy of the unlocking signal. As long as a high level is received, the lock will be unlocked, regardless of whether the high level is sent by the lower computer. Thus, many lawbreakers who understand principles of the electronically controlled lock, connect the electronically controlled lock to a self-made external device to steal the goods by using a defect of inability to determine the legitimacy of the unlocking signal of the electronically controlled lock.

SUMMARY

[0005] The present application aims to solve at least one of the technical problems in the prior art. Therefore, the present application provides a control method for an intelligent vending cabinet, which effectively verifies the legitimacy of an unlocking signal sent to an electronically controlled lock through encrypted communication between the vending cabinet and the electronically

controlled lock, avoids opening of a door by a false external signal, and improves the safety and reliability of the vending cabinet.

[0006] The present application further provides a control device and system for an intelligent vending cabinet, an electronic device, and a storage medium.

[0007] The control method for the intelligent vending cabinet of the present application includes:
determining, by the vending cabinet, that a door opening request is allowed, and sending an encrypted unlocking instruction to an electronically controlled lock provided in the vending cabinet, and opening a door of the vending cabinet after the electronically controlled lock successfully decrypts the unlocking instruction.

[0008] The control method of the intelligent vending cabinet provided in the present application further has the following additional technical features.

[0009] In an embodiment, the method further includes:

obtaining, by the vending cabinet, door lock state information, determining that the door lock state information is non-encrypted, or determining that the door lock state information is not successfully decrypted, and sending an alarm message to a cloud terminal.

[0010] Furthermore, the method further includes:

sending, by the vending cabinet, an alarm message to a cloud terminal, in accordance with a determination that state information of the electronically controlled lock is not obtained within a target time period, and.

[0011] The control method for the intelligent vending cabinet of the present application includes:

obtaining, by an electronically controlled lock, an unlocking instruction;

successfully decrypting the unlocking instruction and opening the door of the vending cabinet.

[0012] The control method for the intelligent vending cabinet of the present application further has the following additional technical features.

[0013] In an embodiment, the method further includes:

obtaining, by the electronically controlled lock, door lock state information, encrypting the door lock state information, and sending the encrypted door lock state information to the vending cabinet, and sending, by the vending cabinet, a settlement request to a cloud terminal after determining that the door lock state information is successfully decrypted.

[0014] Furthermore, after obtaining, by the electronically controlled lock, the unlocking instruction, the method further includes:

determining, by the electronically controlled lock, that the unlocking instruction is non-encrypted, or determining that the unlocking instruction is not successfully decrypted and

continuously maintaining the door of the vending cabinet closed.

[0015] The control device for the intelligent vending cabinet of the present application includes:

a determining module, used to determine that a door opening request is allowed; and

a control module, used to send an encrypted unlocking instruction to an electronically controlled lock provided in the vending cabinet, and to open a door of the vending cabinet after the electronically controlled lock successfully decrypts the unlocking instruction.

[0016] The control device for the intelligent vending cabinet of the present application includes:

an obtaining module, used to obtain an unlocking instruction; and

a control module, used to successfully decrypt the unlocking instruction and open a door of the vending cabinet.

[0017] The control system for the intelligent vending cabinet of the present application includes:

a vending cabinet, used to determine that a door opening request is allowed and send an encrypted unlocking instruction to an electronically controlled lock provided in the vending cabinet; and

an electronically controlled lock, used to successfully decrypt the unlocking instruction and open a door of the vending cabinet.

[0018] Furthermore, the electronically controlled lock is used to obtain door lock state information and send the encrypted door lock state information to the vending cabinet;

the vending cabinet is further used to send a settlement request to a cloud terminal after determining that the lock state information is successfully decrypted.

[0019] The electronic device of the present application includes a memory, a processor, and a computer program stored in the memory and executable in the processor. The computer program, when executed by the processor, causes the processor to implement the steps of the control method for the intelligent vending cabinet as described above.

[0020] In a non-transitory computer-readable storage medium of the present application, a computer program is stored, the computer program, when executed by the processor, causes a processor to implement the steps of the control method for the intelligent vending cabinet as described above.

[0021] The additional aspects and advantages of the present application will be set forth in part which follows, and, in part, will be apparent from the following description, or may be learned by the practice of the present application.

BRIEF DESCRIPTION OF THE DRAWINGS

[0022] To provide a clearer explanation of the embodiments of the present application or the

solutions in the prior art, a brief description is given to the accompanying drawings required in the description of the embodiments or the prior art. The accompanying drawings in the following description are only some embodiments of the present application. For those ordinarily skilled in the art, other accompanying drawings may be obtained based on these drawings without any creative effort.

FIG. 1 is a first schematic flowchart of a control method for an intelligent vending cabinet according to the present application;

FIG. 2 is a second schematic flowchart of the control method for the intelligent vending cabinet according to the present application;

FIG. 3 is a third schematic flowchart of a control method for an intelligent vending cabinet according to the present application;

FIG. 4 is a fourth schematic flowchart of a control method for an intelligent vending cabinet according to the present application;

FIG. 5 is a fifth schematic flowchart of a control method for an intelligent vending cabinet according to the present application;

FIG. 6 is a first schematic structural diagram of a control device for the intelligent vending cabinet according to the present application;

FIG. 7 is a second schematic structural diagram of a control device for an intelligent vending cabinet according to the present application;

FIG. 8 is a third schematic structural diagram of a control device for an intelligent vending cabinet according to the present application;

FIG. 9 is a fourth schematic structural diagram of a control device for an intelligent vending cabinet according to the present application; and

FIG. 10 is a schematic structural diagram of an electronic device according to the present application.

DETAILED DESCRIPTION

[0023] The following provides a further detailed description of the implementation of the present application in conjunction with the accompanying drawings and embodiments. The following embodiments are used to illustrate the present application, but not to limit the scope of the present application.

[0024] FIG. 1 shows a schematic flowchart of a control method for an intelligent vending cabinet according to the present application. As shown in FIG. 1, the method is applicable to an intelligent vending cabinet having a lock-controlled door, the vending cabinet is configured with an

electronically controlled lock capable of controlling the opening of the door. The method, performed by a vending cabinet, includes the following steps:

11, receiving an authentication result sent from a cloud terminal, and determining whether a door opening request is allowed based on the authentication result; and

12, generating an unlocking instruction in an encryption manner after determining that the door opening request is allowed, and sending the unlocking instruction to an electronically controlled lock, and opening a door of the vending cabinet after the electronically controlled lock successfully decrypts the unlocking instruction.

[0025] Regarding steps 11 and 12, it should be noted that, in the present application, various goods are placed in an intelligent vending cabinet, and a user may request to open the door by scanning a quick response (QR) code, and then take the goods.

[0026] The intelligent vending cabinet includes two control systems of which one control system, as an upper computer, interacts with a cloud terminal, and the other control system, as a lower computer, interacts with an electronically controlled lock.

[0027] The user scans the QR code displayed on a display of the vending cabinet using a mobile terminal, that is, actually the mobile terminal sends the door opening request to the cloud terminal, the door opening request including an identification number of the vending cabinet and a payment account of the user in the mobile terminal.

[0028] The cloud terminal sends the authentication result to the upper computer of the vending cabinet based on the door opening request, the authentication result actually allows the user to open the door during the purchase process. After the upper computer determines that the door opening request from the user is allowed based on the authentication result, the upper computer informs the lower computer of the vending cabinet of a message that the request is allowed. The lower computer sends an unlocking instruction to the electronically controlled lock, and the unlocking instruction is sent in an encryption manner.

[0029] The electronically controlled lock decrypts the unlocking instruction after receiving the unlocking instruction. After the unlocking instruction is successfully decrypted, a mechanical apparatus of the electronically controlled lock is controlled to open the door. The user may choose and take the goods inside the machine after the door is opened.

[0030] The control method for the intelligent vending cabinet according to the present application effectively verifies the legitimacy of an unlocking signal of the electronically controlled lock through encrypted communication between the vending cabinet and the electronically controlled lock, avoiding opening of the door by a false external signal, and improving the safety and reliability of the vending cabinet.

[0031] FIG. 2 shows a schematic flowchart of a control method for an intelligent vending cabinet according to the present application. As shown in FIG. 2, the method, performed by a vending cabinet, includes the following steps:

11, receiving an authentication result sent from a cloud terminal, and determining whether a door opening request is allowed based on the authentication result;

12, generating an unlocking instruction in an encryption manner after determining that the door opening request is allowed, and sending the unlocking instruction to an electronically controlled lock, opening a door of the vending cabinet after the electronically controlled lock successfully decrypts the unlocking instruction; and

21, obtaining door lock state information, determining that the door lock state information is non-encrypted, or determining that the door lock state information is not successfully decrypted, and sending an alarm message to the cloud terminal.

[0032] Based on the above, steps 11 and 12 are described in detail and are not repeated here.

[0033] Regarding step 21, it should be noted that, in the present application, after the user takes the goods from the cabinet, the door is closed again and the electronically controlled lock is locked again. Thus, the electronically controlled lock obtains door lock state information in real time, the door lock state information representing whether the door is closed.

[0034] The electronically controlled lock also sends the door lock state information to the lower computer of the vending cabinet in an encryption manner, the lower computer decrypts the door lock state information. After decryption is successfully performed and the door is determined to be closed based on the door lock state information, the lower computer sends the upper computer a signal that the door is closed. The upper computer sends the information of the goods took by the user to the cloud terminal, the cloud terminal completes a settlement process based on information of the goods and the payment account.

[0035] In the present application, the user may false the door lock state information. For example, the user may unplug a communication cable between the electronically controlled lock and the lower computer, and then use an external device to input a false signal into a pin of a socket of the lower computer. The false signal is used to replace a door lock status signal.

[0036] If the false signal is not processed in an encryption manner, when the lower computer determine that the signal is non-encrypted, it indicates that the signal is illegal. The lower computer sends a notification signal that the door may not be closed to the upper computer, and then the upper computer may send the alarm message to the cloud terminal. The alarm message indicates the number of the vending cabinet. The vending cabinet operator may notify the staff to check the scene and solve problems in time to avoid loss of the goods.

[0037] If the false signal is processed in an encryption manner, the lower computer decrypts the encrypted information after determining that the false signal is encrypted. Due to the fact that an encryption protocol is not known from the false signal, the lower computer fails to decrypt the false signal. In this case, the lower computer also sends the notification signal that the door may not be closed to the upper computer, and then the upper computer sends the alarm message to the cloud terminal. The alarm message indicates the number of the vending cabinet. The vending cabinet operator may notify the staff to check the scene and solve problems in time to avoid loss of the goods.

[0038] The control method for the intelligent vending cabinet provided in the present application effectively verifies the legitimacy of the unlocking signal and the door lock state information of the electronically controlled lock through encrypted communication between the vending cabinet and the electronically controlled lock, avoiding the opening and not closing of the door by the false external signal, and improving the safety and reliability of the vending cabinet.

[0039] FIG. 3 shows a schematic flowchart of a control method for an intelligent vending cabinet according to the present application. As shown in FIG. 3, the method, performed by a vending cabinet, includes the following steps:

11, receiving, by a vending cabinet, an authentication result sent from a cloud terminal, and determining whether a door opening request is allowed based on the authentication result;

12, generating an unlocking instruction in an encryption manner after determining that the door opening request is allowed, and sending the unlocking instruction to an electronically controlled lock, opening a door of the vending cabinet after the electronically controlled lock successfully decrypts the unlocking instruction;

21, obtaining door lock state information, determining that the door lock state information is non-encrypted, or determining that the door lock state information is not successfully decrypted, and sending an alarm message to the cloud terminal; and

31, sending the alarm message to the cloud terminal in accordance with a determination that a state information of the electronically controlled lock is not obtained within a target time period.

[0040] Based on the above, steps 11, 12 and 21 are described in detail and are not repeated here.

[0041] Regarding step 31, it should be noted that, in the present application, the electronically controlled lock may send its own state information to the vending cabinet at a preset time interval. The state information indicates the electronically controlled lock is whether damaged or not working. In a case that the electronically controlled lock is damaged on purpose, the electronically controlled lock is unable to provide its own state information to the vending cabinet. Thus, the vending cabinet is unable to receive the state information sent from the electronically controlled

lock within the preset time period, and then it is determined that the electronically controlled lock is damaged on purpose or malfunctioned. The lower computer may send a notification signal that the door is not closed to the upper computer, and the upper computer may then send the alarm message to the cloud terminal. The alarm message indicates the number of the vending cabinet. The vending cabinet operator may notify the staff to check the scene and solve problems in time to avoid loss of the goods.

[0042] The control method for the intelligent vending cabinet according to the present application effectively verifies the legitimacy of the unlocking signal and the door lock state information of the electronically controlled lock through encrypted communication between the vending cabinet and the electronically controlled lock, avoiding the opening and not closing of the door by the false external signal, and improving the safety and reliability of the vending cabinet. In addition, whether the electronically controlled lock is damaged is regularly monitored, thereby ensuring timely finding problems.

[0043] FIG. 4 shows a schematic flowchart of a control method for an intelligent vending cabinet according to the present application. As shown in FIG. 4, the method is applicable to an intelligent vending cabinet having a lock-controlled door, the vending cabinet is configured with an electronically controlled lock that may control the opening of the door. The method, performed by an electronically controlled lock, includes the following steps:

41, obtaining an unlocking instruction;

42, successfully decrypting the unlocking instruction and opening a door of a vending cabinet.

[0044] Regarding steps 41 and 42, it should be noted that, in the present application, when using the above control method, based on information interaction processes between the cloud, the upper computer, the lower computer, and the electronically controlled lock, it may be inferred that the electronically controlled lock may obtain instructions in the following two situations. The two instructions include:

1) an unlocking instruction generated by the lower computer in an encryption manner after determining that a door opening request is allowed; and

2) instructions falsified by others using an external device.

[0045] After receiving the instruction, the electronically controlled lock is required to decrypt the instruction first. The lower computer encrypts the instruction according to a pre-configured encryption protocol, and the electronically controlled lock has a key to decrypt the instruction. Since the false instruction is not encrypted, there is no decryption process, which is equivalent to a decryption failure.

[0046] When the decryption is successful, it indicates that the instruction is legal, the

electronically controlled lock opens the door of the vending cabinet. When the decryption fails, it indicates that the instruction is illegal, the electronically controlled lock maintains the door closed.

[0047] In addition, if someone illegally sends a false instruction directly to the electronically controlled lock, and the preset encryption protocol is not used in a generation process of the false instruction, the electronically controlled lock may determine the false instruction is non-encrypted, and if the false instruction is encrypted, but the electronically controlled lock is unable to decrypt the instruction, then the electronically controlled lock continues to maintain the door of the vending cabinet closed.

[0048] The control method for the intelligent vending cabinet provided in the present application effectively verifies the legitimacy of an unlocking signal of the electronically controlled lock through encrypted communication between the vending cabinet and the electronically controlled lock, avoiding opening of the door by a false external signal, and improving the safety and reliability of the vending cabinet.

[0049] FIG. 5 shows a schematic flowchart of a control method for an intelligent vending cabinet according to the present application. As shown in FIG. 5, the method, performed by an electronically controlled lock, includes the following steps:

41, obtaining an unlocking instruction;

42, successfully decrypting the unlocking instruction and opening a door of a vending cabinet;
and

51, obtaining door lock state information, encrypting the door lock state information, and sending the encrypted door lock state information to the vending cabinet to ensure that the vending cabinet decrypts the door lock state information and sends a settlement request to a cloud terminal.

[0050] Based on the above, steps 41 and 42 are described in detail and are not repeated here.

[0051] Regarding step 51, it should be noted that, in the present application, after the user takes the goods from the machine, the door is closed again and the electronically controlled lock is locked again. Thus, the electronically controlled lock obtains door lock state information in real time, the door lock state information represents whether the door is closed.

[0052] The electronically controlled lock also sends the door lock state information to the lower computer of the vending cabinet in an encryption manner, the lower computer decrypts the door lock state information. After decryption and the door is determined to be closed based on the door lock state information, the lower computer sends the upper computer a signal that the door is closed. The upper computer sends the information of the goods took by the user to the cloud terminal, the cloud terminal completes a settlement process based on information of the goods and the payment account.

[0053] The control method of the intelligent vending cabinet according to the present application effectively verifies the legitimacy of an unlocking signal and the door lock state information of the electronically controlled lock through encrypted communication between the vending cabinet and the electronically controlled lock, avoiding opening of the door by a false external signal, and improving the safety and reliability of the vending cabinet.

[0054] FIG. 6 shows a schematic structural diagram of a control device for an intelligent vending cabinet according to the present application, and the device includes a determining module 61 and a first control module 62.

The determining module 61 is used to receive an authentication result sent from a cloud terminal, and determine whether a door opening request is allowed based on the authentication result;

[0055] The first control module 62 is used to send an unlocking instruction to an electronically controlled lock provided in the vending cabinet after determining that the door opening request is allowed, and the electronically controlled lock may successfully decrypt the unlocking instruction and open a door of the vending cabinet.

[0056] In a further device of the above embodiment, the device further includes an alarm module, used to:

obtain door lock state information, determine that the door lock state information is non-encrypted, or determine that the door lock state information is not successfully decrypted, and send an alarm message to the cloud terminal.

[0057] In a further apparatus of the above embodiment, the alarm module is further used to:

determine that state information of the electronically controlled lock is not obtained within a preset time period, and send the alarm message to the cloud.

[0058] As the principle of the apparatus in the present application is the same as that of the method of the above embodiments, more detailed description is not repeated here.

[0059] It should be noted that, in the present application, relevant functional modules may be implemented through a hardware processor.

[0060] The control device for the intelligent vending cabinet provided in the present application effectively verifies the legitimacy of an unlocking signal of the electronically controlled lock through encrypted communication between the vending cabinet and the electronically controlled lock, avoiding opening of the door by a false external signal, and improving the safety and reliability of the vending cabinet.

[0061] FIG. 7 shows a schematic structural diagram of a control device for an intelligent vending cabinet according to the present application. The device includes a determining module 61, a first

control module 62, and an alarm module 71.

The determining module 61 is used to receive an authentication result sent from a cloud terminal, and determine whether a door opening request is allowed based on the authentication result.

[0062] The first control module 62 is used to send an unlocking instruction in an encryption manner to an electronically controlled lock provided in the vending cabinet after determining that the door opening request is allowed, and the electronically controlled lock may successfully decrypt the unlocking instruction and open a door of the vending cabinet.

[0063] The alarm module 71 is used to:

obtain door lock state information, determine that the door lock state information is non-encrypted, or determine that the door lock state information is not successfully decrypted, and send an alarm message to the cloud terminal.

[0064] The alarm module 71 is further used to:

determine that state information of the electronically controlled lock is not obtained within a preset time period, and send the alarm message to the cloud terminal.

[0065] As the principle of the apparatus in the present application is the same as that of the method of the above embodiments, more detailed description is not repeated here.

[0066] It should be noted that, in the present application, relevant functional modules may be implemented through a hardware processor.

[0067] The control device of the intelligent vending cabinet provided in the present application effectively verifies the legitimacy of an unlocking signal and the door lock state information of the electronically controlled lock through encrypted communication between the vending cabinet and the electronically controlled lock, avoiding opening of the door by a false external signal, and improving the safety and reliability of the vending cabinet.

[0068] FIG. 8 shows a schematic structural diagram of a control device for the intelligent vending cabinet according to the present application. The device includes an obtaining module 81 and a second control module 82 in which

the obtaining module 81 is used to obtain an unlocking instruction; and

the second control module 82 is used to successfully decrypt the unlocking instruction and open a door of a vending cabinet.

[0069] In a further device of the above embodiment, the control module is further used to:

determine that the unlocking instruction is non-encrypted, or determine that the unlocking instruction is not decrypted and continue to maintain the door of the vending cabinet closed.

[0070] As the principle of the device in the present application is the same as that of the method

of the above embodiments, more detailed description is not repeated here.

[0071] It should be noted that, in the present application, relevant functional modules may be implemented through a hardware processor.

[0072] The control device for the intelligent vending cabinet provided in the present application effectively verifies the legitimacy of an unlocking signal of the electronically controlled lock through encrypted communication between the vending cabinet and the electronically controlled lock, avoiding opening of the door by a false external signal, and improving the safety and reliability of the vending cabinet.

[0073] FIG. 9 shows a schematic structural diagram of a control device for the intelligent vending cabinet according to the present application. The device includes an obtaining module 81, a second control module 82, and a reporting module 91 in which:

the obtaining module 81 is used to obtain an unlocking instruction; and

the second control module 82 is used to successfully decrypt the unlocking instruction and open a door of the vending cabinet.

[0074] The control module is further used to:

determine that the unlocking instruction is non-encrypted, or determine that the unlocking instruction is not decrypted and continue to maintain the door of the vending cabinet closed.

[0075] The reporting module 91 is used to:

obtain door lock state information and send the encrypted door lock state information to the vending cabinet, the vending cabinet sends a settlement request to the cloud after the vending cabinet determines that the door lock state information is decrypted.

[0076] As the principle of the device in the present application is the same as that of the method of the above embodiments, more detailed description is not repeated here.

[0077] It should be noted that, in the present application, relevant functional modules may be implemented through a hardware processor.

[0078] The control device for the intelligent vending cabinet according to the present application effectively verifies the legitimacy of an unlocking signal and the door lock state information of the electronically controlled lock through encrypted communication between the vending cabinet and the electronically controlled lock, avoiding opening of the door by a false external signal, and improving the safety and reliability of the vending cabinet.

[0079] FIG. 10 illustrates a schematic structural diagram of an electronic device. As shown in FIG. 10, the electronic device may include: a processor 101, a communication interface 102, a memory 103, and a communication bus 104, where the processor 101, the communication interface 102, and the memory 103 communicate with each other through the communication bus

104. The processor 101 may invoke a logical instruction in the memory 103 to execute the following method: receiving an authentication result sent from a cloud terminal, and determining whether a door opening request is allowed based on the authentication result; generating an unlocking instruction in an encryption manner after determining that the door opening request is allowed, and sending the unlocking instruction to an electronically controlled lock, enabling the electronically controlled lock to open a door after decrypting the unlocking instruction.

[0080] In addition, when the logical instruction in the memory 103 mentioned above may be implemented in a form of software functional unit and sold or used as an independent product, the logical instruction may be stored in a computer readable storage medium. Based on such interpretation, the solution of the present application, in essence, or the portion that contributes to the prior art or the portion of the solution, may be implemented in a form of a software product, the software product being stored in a storage medium. The storage medium includes several instructions to enable a computer device (which may be a personal computer, a server, or a network device, etc.) to perform all or part of the steps of the method described in various embodiments of the present application. The aforementioned storage media include: various media that may store program codes, such as USB flash drives, removable hard drives, read-only memory (ROM), random access memory (RAM), magnetic disks, or optical disks.

[0081] The embodiments of the present application also provide a non-transitory computer-readable storage medium, and a computer program is stored on the storage medium. The computer program is implemented by a processor to execute the method provided in the above embodiments, for example: receiving an authentication result sent from a cloud terminal, and determining whether a door opening request is allowed based on the authentication result; generating an unlocking instruction in an encryption manner after determining that the door opening request is allowed, and sending the unlocking instruction to an electronically controlled lock, and opening a door of the vending cabinet after the electronically controlled lock decrypts the unlocking instruction.

[0082] The present application provides an electronic device, and the electronic device may include: a processor, a communication interface, a memory, and a communication bus, where the processor, the communication interface, and the memory communicate with each other through the communication bus. The processor may invoke a logical instruction in the memory to execute the following method: obtaining an unlocking instruction; decrypting the unlocking instruction and open a door of the vending cabinet.

[0083] In addition, when the logical instruction in the memory mentioned above may be implemented in a form of software functional unit and sold or used as an independent product, the

logical instruction may be stored in a computer readable storage medium. Based on such interpretation, the solution of the present application, in essence, or the portion that contributes to the prior art or the portion of the solution, may be implemented in a form of a software product, the software product is stored in a storage medium. The storage medium includes several instructions to enable a computer device (which may be a personal computer, a server, or a network device, etc.) to perform all or part of the steps of the method described in various embodiments of the present application. The aforementioned storage media include: various media that may store program codes, such as USB flash drives, removable hard drives, read-only memory (ROM), random access memory (RAM), magnetic disks, or optical disks.

[0084] The present application also provides a non-transitory computer-readable storage medium, a computer program being stored on the storage medium. The computer program is implemented by a processor to execute the method provided in the above embodiments, for example: obtaining an unlocking instruction; decrypting the unlocking instruction and controlling to open a door of the vending cabinet.

[0085] Through the description of the above embodiments, those skilled in the art may clearly understand that each embodiment may be achieved through a software and a necessary universal hardware platform, and each embodiment may also be achieved through a hardware. Based on such interpretation, the solution of the present application, in essence, or the portion that contributes to the prior art, may be implemented in a form of a software product, which may be stored in computer readable storage media such as ROM/RAM, magnetic disks, optical disks, etc, the media including several instructions to enable a computer device (which may be a personal computer, a server, or a network device, etc.) to execute the method described in various embodiments or certain parts of the embodiments.

[0086] Finally, it should be noted that the above embodiments are only used to illustrate the solution of the present application, not to limit it; although the present application is described in detail with reference to the aforementioned embodiments, those ordinarily skilled in the art should understand: they may still modify the solutions recorded in the aforementioned embodiments, or equivalently replace some of the technical features; and these modifications or replacements do not separate the essence of the corresponding solutions from the spirit and scope of the solutions of the various embodiments of the present application.

WHAT IS CLAIMED IS:

1. A control method for an intelligent vending cabinet, comprising:
determining, by the vending cabinet, that a door opening request is allowed, and sending an encrypted unlocking instruction to an electronically controlled lock provided in the vending cabinet, opening a door of the vending cabinet after the electronically controlled lock successfully decrypts the unlocking instruction.
2. The control method for the intelligent vending cabinet of claim 1, further comprising:
obtaining, by the vending cabinet, door lock state information, determining that the door lock state information is non-encrypted, or determining that the door lock state information is not successfully decrypted, and sending an alarm message to a cloud terminal.
3. The control method for the intelligent vending cabinet of claim 1, further comprising:
sending, by the vending cabinet, the alarm message to a cloud terminal in accordance with a determination that state information of the electronically controlled lock is not obtained within a target time period.
4. A control method for an intelligent vending cabinet, comprising:
obtaining, by an electronically controlled lock, an unlocking instruction;
decrypting the unlocking instruction and opening a door of the vending cabinet.
5. The control method for the intelligent vending cabinet of claim 4, further comprising:
obtaining, by the electronically controlled lock, door lock state information, encrypting the door lock state information, and sending the encrypted door lock state information to the vending cabinet, sending a settlement request to a cloud after the vending cabinet determines that the door lock state information is decrypted.
6. The control method for the intelligent vending cabinet of claim 4, wherein after obtaining, by the electronically controlled lock, the unlocking instruction, the method further comprises:
determining, by the electronically controlled lock, that the unlocking instruction is non-encrypted, or determining that the unlocking instruction is not successfully decrypted, and continuously maintaining the door of the vending cabinet closed.
7. A control device for an intelligent vending cabinet, comprising:
a determining module, configured to determine that a door opening request is allowed; and
a control module, configured to send an encrypted unlocking instruction to an electronically controlled lock provided in the vending cabinet, to open a door of the vending cabinet after the electronically controlled lock successfully decrypts the unlocking instruction.
8. A control device for an intelligent vending cabinet, comprising:

an obtaining module, configured to obtain an unlocking instruction; and
a control module, configured to successfully decrypt the unlocking instruction and open a door of the vending cabinet.

9. A control system for an intelligent vending cabinet, comprising:

a vending cabinet, configured to determine that a door opening request is allowed and send an encrypted unlocking instruction to an electronically controlled lock provided in the vending cabinet; and

an electronically controlled lock, configured to successfully decrypt the unlocking instruction and open a door of the vending cabinet.

10. The control system of the intelligent vending cabinet of claim 9, wherein the electronically controlled lock is further configured to obtain door lock state information and send the encrypted door lock state information to the vending cabinet;

the vending cabinet is further configured to send a settlement request to a cloud terminal after determining that the lock state information is successfully decrypted.

11. An electronic device comprising a memory, a processor, and a computer program stored in the memory and executable in the processor, wherein the computer program, when executed by the processor, causes the electronic device to implement the steps of the control method for an intelligent vending cabinet according to any one of claims 1 to 3, or to implement the steps of the control method for an intelligent vending cabinet according to any one of claims 4 to 6.

12. A non-transitory computer-readable storage medium, having a computer program stored thereon, wherein the computer program, when executed by a processor, causes the processor to implement the steps of the control method for an intelligent vending cabinet according to any one of claims 1 to 3, or to implement the steps of the control method for an intelligent vending cabinet according to any one of claims 4 to 6.