

PAYMENT SECURITY MANAGEMENT METHOD AND APPARATUS, AND PAYMENT SYSTEM

TECHNICAL FIELD

[0001] This disclosure relates to the field of blockchain technologies, and specifically, to a
5 payment security management method and apparatus, and a payment system.

BACKGROUND

[0002] When an Internet of Things machine is used to make a payment, it cannot be learned
whether a result page displayed by the Internet of Things machine is accurate.

SUMMARY

10 [0003] In view of this, this disclosure provides a payment security management method and
apparatus, and a payment system.

[0004] According to a first aspect, a payment security management method is provided, and is
applied to a payment system. The payment system includes an Internet of Things machine and a
serving end. The Internet of Things machine is configured to send a payment request to the serving
15 end. The serving end is configured to respond to the payment request. The method includes:
obtaining first payment data, where the first payment data is generated based on clearing data
corresponding to the payment request; obtaining second payment data, where the second payment
data is generated based on a result page corresponding to the payment request, and the result page
is used by the Internet of Things machine for display to the outside; and performing consistency
20 comparison between the first payment data and the second payment data, to obtain a comparison
result.

[0005] Optionally, in some embodiments, the serving end includes an Internet of Things
machine serving end and a payment serving end, and the clearing data includes acquiring data at
the Internet of Things machine serving end and/or settlement data at the payment serving end.

25 [0006] Optionally, in some embodiments, the payment serving end includes unified payment.

- [0007] Optionally, in some embodiments, after the obtaining a comparison result, the method further includes: storing the comparison result when the comparison result is "inconsistent".
- [0008] Optionally, in some embodiments, after the obtaining a comparison result, the method further includes: intercepting the payment request when the comparison result is "inconsistent".
- 5 [0009] Optionally, in some embodiments, the first payment data and the second payment data include information flow data and/or fund flow data corresponding to the payment request.
- [0010] According to a second aspect, a payment security management apparatus is provided, and is applied to a payment system. The payment system includes an Internet of Things machine and a serving end. The Internet of Things machine is configured to send a payment request to the
10 serving end. The serving end is configured to respond to the payment request. The apparatus includes: a first obtaining unit, configured to obtain first payment data, where the first payment data is generated based on clearing data of the payment request; a second obtaining unit, configured to obtain second payment data, where the second payment data is generated based on a result page of the payment request, and the result page is used by the Internet of Things machine
15 for display to the outside; and a comparison unit, configured to perform consistency comparison between the first payment data and the second payment data, to obtain a comparison result.
- [0011] Optionally, in some embodiments, the serving end includes an Internet of Things machine serving end and a payment serving end, and the clearing data includes acquiring data at the Internet of Things machine serving end and/or settlement data at the payment serving end.
- 20 [0012] Optionally, in some embodiments, the payment serving end includes unified payment.
- [0013] Optionally, in some embodiments, the apparatus further includes a storage unit, configured to: after the comparison result is obtained, store the comparison result when the comparison result is "inconsistent".
- [0014] Optionally, in some embodiments, the apparatus further includes an interception unit,
25 configured to: after the comparison result is obtained, intercept the payment request when the comparison result is "inconsistent".
- [0015] Optionally, in some embodiments, the first payment data and the second payment data include an information flow and/or a fund flow corresponding to the payment request.
- [0016] According to a third aspect, a payment system is provided, and includes: an Internet of
30 Things machine, configured to send a payment request to a serving end; the serving end, configured to process the payment request to generate payment result data; and a platform,

configured to perform the following operations: obtaining first payment data, where the first payment data is generated based on clearing data of the payment request; obtaining second payment data, where the second payment data is generated based on a result page corresponding to the payment request, and the result page is used by the Internet of Things machine for display to the outside; and performing consistency comparison between the first payment data and the second payment data, to obtain a comparison result.

[0017] According to a fourth aspect, a payment security management apparatus is provided, and includes: a memory, configured to store instructions; and a processor, configured to execute the instructions stored in the memory, to perform the method according to the first aspect.

10 [0018] According to a fifth aspect, a computer-readable storage medium is provided. The computer-readable storage medium stores executable code, and when the executable code is executed, the method according to the first aspect can be implemented.

[0019] According to a sixth aspect, a computer program product is provided, and includes executable code. When the executable code is executed, the method according to the first aspect can be implemented.

15 [0020] According to the payment security management method provided in the embodiments of this disclosure, a clearing result of the payment request and a payment result used by the Internet of Things machine for display to the outside are compared, so that it can be automatically monitored whether a result page displayed at an Internet of Things machine end for each payment is accurate.

BRIEF DESCRIPTION OF DRAWINGS

[0021] FIG. 1 is a schematic diagram of a payment procedure of a payment system in a related technology;

[0022] FIG. 2 is a schematic flowchart of a payment security management method according to an embodiment of this disclosure;

[0023] FIG. 3 is a schematic flowchart of a payment security management method according to another embodiment of this disclosure;

[0024] FIG. 4 is a schematic diagram of a structure of a payment security management apparatus according to an embodiment of this disclosure;

[0025] FIG. 5 is a schematic diagram of a payment system according to an embodiment of this disclosure; and

[0026] FIG. 6 is a schematic diagram of a structure of a payment security management apparatus according to another embodiment of this disclosure.

5

DESCRIPTION OF EMBODIMENTS

[0027] The following clearly and comprehensively describes technical solutions in the embodiments of this disclosure. Clearly, the described embodiments are merely some rather than all of the embodiments of this disclosure.

[0028] With rapid development of Internet of Things technologies, Internet of Things machines based on the Internet of Things technologies develop rapidly. More than tens of millions of payments are made by using the Internet of Things machines per day.

[0029] FIG. 1 is a schematic diagram of a payment procedure of a payment system in a related technology. The payment system shown in FIG. 1 can include an Internet of Things machine 110 and a serving end 120.

[0030] The Internet of Things machine 110 can be configured to provide a payment channel. A user can perform a payment operation through the payment channel provided by the Internet of Things machine 110. The Internet of Things machine 110 can also be referred to as an Internet of Things device, an IoT device, a payment device, a device, an IoT machine, a payment machine, a machine, a payment terminal, or the like.

[0031] As shown in FIG. 1, in step S101, the Internet of Things machine 110 sends a payment request to the serving end 120. The payment request can be, for example, a payment request of the user.

[0032] The Internet of Things machine 110 can provide a payment method such as face scanning or two-dimensional code scanning for the user. A facial feature or a two-dimensional code of the user can be scanned by the Internet of Things machine 110 to complete a payment operation.

[0033] After obtaining a payment message of the user, the Internet of Things machine 110 can send the payment request to the serving end 120 based on the payment message.

[0034] In step S102, the serving end 120 processes the payment request. That the serving end

120 processes the payment request can include: analyzing the payment request; and completing fund transfer based on the payment request. For example, the serving end 120 can deduct 10 yuan from an Alipay account of a user A based on the payment request, and add 10 yuan to an Alipay account of a merchant B.

5 **[0035]** It should be understood that actually, an account used by a user or a merchant can be any account. For example, an account of the user A can be a Yu'E Bao account provided by Alipay, or can be a bank card account provided by a bank (for example, Construction Bank).

[0036] In step S103, the serving end 120 sends a result page to the Internet of Things machine 110 based on a processing result of the payment request. The result page can also be referred to as
10 result page data. The result page can include data required for the Internet of Things machine to display.

[0037] In step S104, the Internet of Things machine 110 can display the result page.

[0038] The Internet of Things machine 110 can display the result page in a plurality of manners. A specific manner of displaying the result page is not limited in this disclosure. For example, the
15 result page can be displayed to the user in a form of a page. For another example, the result page can be displayed to the user in a voice broadcast manner.

[0039] The result page sent by the serving end 120 can include information related to an information flow and a fund flow. For example, the result page sent by the serving end 120 can
20 include a user ID, a transaction number, a payment channel, a payment status, and a payment amount.

[0040] The Internet of Things machine 110 can obtain, in a plurality of manners, data required for the to-be-displayed result page. For example, all of the data required for the to-be-displayed
result page can be calculated by the serving end 120 and transmitted to the Internet of Things machine 110.

25 **[0041]** For another example, the data required for the to-be-displayed result page can be jointly generated by the serving end 120 and the Internet of Things machine 110. For example, the Internet of Things machine 110 can calculate some data required for generating the result page, and the serving end 120 can calculate the other data required for generating the result page. The Internet of Things machine 110 summarizes the data required for display, generates the result page, and
30 displays the result page to the outside.

[0042] It can be learned from the above-mentioned procedure description that a payment

request needs to be processed at least by the Internet of Things machine 110 and the serving end 120. The Internet of Things machine 110 and the serving end 120 are usually located at different geographical locations, and information needs to be transferred in a wired or wireless communication manner.

5 **[0043]** In an information transfer process, transferred information may deviate from original information due to various reasons. For example, due to a network problem, the data on the result page displayed by the Internet of Things machine 110 may be inconsistent with data actually stored by the serving end.

10 **[0044]** For another example, information may be tampered with in a transfer process. Consequently, information on the result page finally displayed to the user is inconsistent with actual payment information. For example, the user completes a payment of 20 yuan, and a payment channel is face scanning payment. However, because information is tampered with in a payment process, a payment result displayed by the Internet of Things machine 110 is that the user pays 200 yuan, and the payment channel is two-dimensional code scanning payment. That is, after the
15 user makes a payment, a payment channel and an amount displayed by the Internet of Things machine 110 are inconsistent with an amount finally paid.

20 **[0045]** For another example, a settlement unit used by the serving end 120 and a settlement unit used by the Internet of Things machine 110 may be different, resulting in a difference in an amount finally displayed by the Internet of Things machine 110. For example, after the user makes a payment, the merchant issues a 10-cent coupon to the user on the result page for next consumption. However, the Internet of Things machine 110 displays the 10-cent coupon as 10 yuan.

25 **[0046]** That is, for an Internet of Things-based payment system with a large quantity of payments (for example, more than tens of millions of payments made through face scanning per day), a payment result displayed by the Internet of Things machine 110 to the outside may be inconsistent with payment data delivered or stored by the serving end 120.

30 **[0047]** When the data displayed on the result page is inconsistent with the actual payment data, a loss may be caused to funds of the user or the merchant. In a severe case, the company's reputation may be damaged.

30 **[0048]** Data provided by the serving end is usually reliable. Therefore, it can be ensured that a payment result provided by the Internet of Things machine is consistent with an actual payment

result of the user, provided that it is ensured that data related to the result page used at an Internet of Things machine end for display is correct. That is, it can be ensured that what the user sees is what the user obtains.

[0049] To ensure that what the user sees is what the user obtains, the result page data at the Internet of Things machine end and the data at the serving end usually need to be compared. If there is inconsistency in a comparison result, it indicates that there is a problem in an execution process of the payment request. That is, what the user sees may be different from a final payment result.

[0050] In a payment verification method provided in a related technology, consistency comparison is usually performed by pulling data stored in a storage system.

[0051] However, because there are a large quantity of transactions (for example, a large quantity of payment requests) at the Internet of Things machine end, and there is no need to store transaction information at the Internet of Things machine end, a storage system (for example, a database) is usually not configured at the Internet of Things machine end.

[0052] The Internet of Things machine without a storage system cannot perform data correctness verification in a common automatic verification manner. Therefore, in the payment system using the Internet of Things machine, payment correctness is currently still ensured through manual reconciliation.

[0053] Manual reconciliation can be completed in a plurality of manners. For example, the merchant actively applies for a bill to a provider of the Internet of Things machine, and the merchant manually verifies the bill.

[0054] For another example, because there are many merchants that use the Internet of Things machine, a provider of the Internet of Things machine usually cooperates with an ISV organization, and the ISV organization provides the Internet of Things machine for the merchant, and manages the merchant that uses the Internet of Things machine. The merchant can apply for reconciliation to the ISV organization. The ISV organization can collect reconciliation information of the merchant, and provide a bill to the ISV organization.

[0055] In the above-mentioned two reconciliation manners, reconciliation is essentially manually completed. It can be understood that in the manual reconciliation manner, reconciliation efficiency is low, a labor demand is high, and costs are high.

[0056] In addition, there are an excessively large quantity of payments in the Internet of

Things-based payment system, and there are many types of Internet of Things machines with wide coverage. Therefore, it is difficult to manually monitor each payment request that passes through the Internet of Things-based payment system.

[0057] In conclusion, it can be learned that how to effectively monitor correctness of each payment is a current challenge for the payment system that uses the Internet of Things machine.

[0058] To resolve the above-mentioned problem, this disclosure provides a payment security management method, to efficiently monitor correctness of each payment, so as to improve security of a payment system.

[0059] With reference to FIG. 2, the following describes in detail the payment security management method provided in the embodiments of this disclosure.

[0060] FIG. 2 is a schematic flowchart of a payment security management method according to an embodiment of this disclosure. The payment security management method shown in FIG. 2 can be applied to a payment system. The payment system can be a system used for a payment. Funds can be transferred through the payment system.

[0061] For example, if a user purchases a commodity worth 10 yuan from a merchant, the user can pay the merchant through the payment system. The payment system can process the transaction, deduct 10 yuan from an account of the user, and add 10 yuan to an account of the merchant.

[0062] The payment system can include an Internet of Things machine and a serving end. The Internet of Things machine can provide a payment channel to the outside. For example, the Internet of Things machine can accept a payment request of the user. For another example, the Internet of Things machine can send a payment request to the serving end. For another example, the Internet of Things machine can receive a payment result corresponding to a payment request from the serving end.

[0063] The serving end can be a serving apparatus configured to interact with the Internet of Things machine to complete payment processing. The serving end can be configured to respond to the payment request sent by the Internet of Things machine. The responding to the payment request sent by the Internet of Things machine can include: completing fund transfer based on information in the payment request.

[0064] A specific implementation form of the serving end is not limited in this disclosure. For example, the serving end can include a server or a computer that can provide a service to the outside.

- [0065] With reference to FIG. 2, in step S210, first payment data is obtained. The first payment data can be generated based on clearing data corresponding to the payment request.
- [0066] The first payment data can be obtained in a plurality of manners. For example, an obtaining request can be actively initiated to the serving end. After receiving the obtaining request, the serving end provides the first payment data.
- [0067] For another example, the first payment data can be directly obtained from the serving end. For example, direct obtaining can be implemented by embedding a point at the serving end. A point can be embedded at the serving end in a plurality of manners. For example, an SDK can be set at the serving end.
- 10 [0068] The first payment data can be generated based on the clearing data corresponding to the payment request in a plurality of manners. For example, the clearing data corresponding to the payment request can be directly used as the first payment data.
- [0069] For another example, some data in the clearing data of the payment request can be obtained as the first payment data. The some data can include, for example, data related to a fund element. The fund element can include, for example, fund-related data such as a user ID, a payment amount, and a payment status.
- 15 [0070] The clearing data can be generated by the serving end in the payment system. The clearing data can include information flow data and/or fund flow data related to the payment request.
- 20 [0071] The information flow can also be referred to as a data flow. The information flow data can include, for example, data related to the Internet of Things machine (for example, an SN code and a MAC code of the Internet of Things machine) and a payment method (for example, face scanning payment or two-dimensional code payment) of the user. The fund flow data can include, for example, a user ID, a transaction number, a payment channel, a payment status, and a payment amount.
- 25 [0072] In some embodiments, the serving end can store the clearing data. The serving end can store the clearing data in a plurality of manners. For example, the serving end can store the clearing data in a form of a document.
- [0073] In some embodiments, the serving end can be connected to a storage system. The clearing data can be stored in the storage system in a form of a document. The storage system can be, for example, a database.
- 30

[0074] In step S220, second payment data is obtained. The second payment data can be generated based on a result page corresponding to the payment request. The result page is used by the Internet of Things machine for display to the outside.

[0075] The second payment data can be obtained in a plurality of manners. For example, the second payment data can be directly obtained from the serving end.

[0076] For another example, after receiving the payment result, the Internet of Things machine can actively report the second payment data.

[0077] For another example, the second payment data can be directly captured from the Internet of Things machine. A capture manner can be, for example, embedding a point in the Internet of Things machine. For example, a point can be embedded in the Internet of Things machine by setting a corresponding SDK in the Internet of Things machine.

[0078] The result page can be used by the Internet of Things machine for display to the outside. It should be understood that use of the result page to describe a page that displays the payment result to the user is merely intended to make the description clearer. For example, the result page can refer to data related to the result page, or can be a page that can be displayed on a display screen, or display information (for example, voice broadcast information) displayed in another form.

[0079] For example, for an Internet of Things machine (for example, a dragonfly machine) with a display screen, the result page can refer to a payment result displayed on the display screen of the Internet of Things machine. For another example, for an Internet of Things machine (for example, a small white box machine) with a play module, the result page can refer to a voice broadcast result of the Internet of Things machine.

[0080] Content displayed on the result page can be randomly set based on an actual requirement. Specific content displayed on the result page is not limited in this disclosure. For example, the result page can display a payment amount, a user ID, and a payment status (for example, payment success or payment failure) to the user.

[0081] In some embodiments, the result page can further include an advertisement placed by the merchant. The advertisement placed by the merchant can include any type of advertisement. For example, the advertisement placed by the merchant can include shopping mall promotion information and restaurant discount information. For another example, the advertisement placed by the merchant can include a coupon that can be used for next consumption.

[0082] The second payment data can be generated based on the result page corresponding to the payment request in a plurality of manners. For example, the result page corresponding to the payment request can be directly used as the second payment data.

[0083] For another example, some data on the result page corresponding to the payment request can be used as the second payment data. The some data on the result page can include, for example, data related to a fund element. The data related to the fund element can include, for example, a user ID, a payment amount, and a payment status.

[0084] In step S230, consistency comparison is performed between the first payment data and the second payment data, to obtain a comparison result.

10 [0085] The first payment data and the second payment data can include same data. For example, both the first payment data and the second payment data can include fund flow data and/or information flow data.

[0086] The fund flow data can include, for example, a user ID, a transaction number, a payment channel, a payment status, and an amount. The information flow data can include, for example, data related to the Internet of Things machine (for example, an SN code and a MAC code of the Internet of Things machine) and a payment method (for example, face scanning payment or two-dimensional code payment) of the user.

15 [0087] Consistency comparison can mean that data items included in the first payment data and data items included in the second payment data are compared one by one, to determine whether the data is exactly the same.

20 [0088] For example, the first payment data and the second payment data can include information such as a user ID, a transaction number, a payment amount, a payment method, a payment status, and a device code of the Internet of Things device.

[0089] The above-mentioned data items in the first payment data and the second payment data are compared one by one. For example, it is determined, through comparison, whether there is a same user ID, a same transaction number, and a same payment amount.

25 [0090] Provided that there is a difference in any data item in all the compared data items, it is considered that the first payment data and the second payment data are inconsistent.

[0091] When the first payment data and the second payment data are inconsistent, it indicates that the clearing data stored at the serving end is inconsistent with the data on the result page displayed by the Internet of Things machine to the outside.

30

[0092] A data comparison mechanism is added to the payment system, so that each payment request in the payment system that uses the Internet of Things machine can be monitored. Further, according to the method provided in this disclosure, an incorrect payment request can be found in a timely manner on the result page displayed by the Internet of Things machine, and correctness of each payment in the payment system can be automatically monitored.

[0093] When the comparison result is "inconsistent", it usually indicates that the payment system is vulnerable. Therefore, to improve robustness of the payment system, the comparison result can be further processed when the comparison result is "inconsistent".

[0094] For example, when the comparison result is "inconsistent", the comparison result that is "inconsistent" can be stored. The comparison result can be presented in a form of a log. Therefore, the storing the comparison result can mean storing a comparison log generated in a comparison process.

[0095] The comparison result can be stored in a plurality of manners. For example, the comparison result can be stored in storage space (for example, a hard disk of the computer or the server). For another example, the comparison result can be printed.

[0096] The result that is "inconsistent" is stored, to help a software practitioner (for example, a software development or operation and maintenance person) locate a problem in the system and improve problem processing efficiency.

[0097] For another example, when the comparison result is "inconsistent", alarm information can be configured for a scenario in which inconsistency is found through comparison. When a scenario corresponding to a payment request is consistent with the scenario for which the alarm information is configured, the alarm information can be sent.

[0098] For example, a unit used by the Internet of Things machine to display the result page is yuan, and a unit used by the serving end to store the settlement data is cent. If there is a logical problem in the payment system, an error may be caused to the result page displayed by the Internet of Things machine. For example, 0.1 yuan should be displayed (the unit for storage at the serving end is cent, that is, the data 10 cents stored at the serving end should be displayed as 0.1 yuan), but a result is that 10 yuan is displayed.

[0099] Alarm information can be configured for this scenario. When a scenario with a unit conversion error is encountered again, the configured alarm information can be triggered.

[0100] A software practitioner can troubleshoot the payment system based on the stored

comparison result or the configured alarm information, to fix vulnerabilities in the payment system, improve system robustness, and enhance security of a payment process.

[0101] In some embodiments, to further improve security of the payment system, the payment can be intercepted when the comparison result is "inconsistent". An incorrect payment request is intercepted in real time, to ensure fund security of the user.

[0102] Because a problematic payment request is intercepted, it is ensured that the result page obtained by the user from the Internet of Things machine is consistent with actual payment information. That is, it is ensured that what the user sees is what the user obtains.

[0103] In some embodiments, a combination of the above-mentioned methods can be used. For example, when the comparison result is "inconsistent", the comparison result that is "inconsistent" can be printed. When a scenario corresponding to the comparison result that is "inconsistent" is a severe scenario, the payment request corresponding to the comparison result is intercepted. When a scenario in which the comparison result is "inconsistent" is a non-severe scenario, only alarm information can be configured for the result, and the payment request is not intercepted.

[0104] Whether a scenario is a severe scenario can be set based on an actual service requirement. For example, the severe scenario can include a scenario in which a corresponding payment amount in the payment result data to be displayed on the result page is completely different from a corresponding payment amount in the clearing data at the serving end.

[0105] According to the method provided in this disclosure, it can be automatically determined, through comparison, whether the result page corresponding to the payment request is consistent with the clearing data (for example, acquiring data) at the serving end. If there is inconsistency, an alarm can be given or interception can be performed for the payment request with inconsistency. Therefore, the method provided in this disclosure implements automatic inspection and an alarm given in seconds.

[0106] In some embodiments, the serving end can include a plurality of different serving ends. Different serving ends can be provided by different operators. Different serving ends can be configured to process different operations in the payment process.

[0107] In some embodiments, the serving end can include an Internet of Things machine serving end and a payment serving end. It should be understood that in addition to the Internet of Things machine serving end and the payment serving end, the serving end can further include

another serving end configured to provide a service. Types and a quantity of serving ends specifically included in the serving end are not limited in this disclosure.

[0108] Each serving end can be implemented in a plurality of manners. For example, the serving end can provide a service to the outside by using the server. Each serving end can include
5 any quantity of servers. A specific implementation form of the serving end or a quantity of servers included in the serving end is not limited in this disclosure.

[0109] The payment serving end can be configured to perform settlement based on the payment request. For example, the payment serving end can complete payment clearing deduction. For another example, the payment serving end can generate a clearing document.

10 **[0110]** In some embodiments, the payment serving end can be connected to a storage system. The storage system can include a database. The payment serving end can store related data in the storage system. The related data can include, for example, payment clearing deduction information or a clearing document. The payment clearing deduction information or the clearing document can include, for example, account information of the user and payment settlement information.

15 **[0111]** In some embodiments, the payment serving end can include unified payment. Unified payment can refer to a payment service system established on core payment software. Unified payment can implement functions such as comprehensive service management, user management, accounting party management, and payer management. Unified payment can provide a secure and efficient payment support environment for a plurality of service systems.

20 **[0112]** The purpose of unified payment is to establish a system for payment and recharging between a payer (a bank or another payment system) and an accounting party (a full-service operation support system).

[0113] The Internet of Things machine serving end can be configured to: receive the payment request sent by the Internet of Things machine, and forward the payment request to the payment
25 serving end.

[0114] After receiving the payment result, the Internet of Things machine serving end can process the payment result to generate the result page used for the Internet of Things machine. The user can view the payment result based on the result displayed by the Internet of Things machine. The user can refer to a consumer making a payment to a merchant, or can refer to a merchant using
30 the Internet of Things machine as a collection tool.

[0115] In some embodiments, the Internet of Things machine serving end can generate

acquiring data based on the payment request. The acquiring data can include a user ID, a transaction number, a payment channel, a payment status, and the like corresponding to the payment request.

[0116] In some embodiments, the clearing data can include the acquiring data at the Internet of Things machine serving end and/or the settlement data at the payment serving end. The first payment data can be generated based on the clearing data.

[0117] The first payment data can include the settlement data at the payment serving end. The settlement data at the payment serving end is usually correct. Therefore, by performing consistency comparison between the second payment data and the first payment data including the settlement data at the payment serving end, it can be quickly determined whether the payment result data on the result page generated by the Internet of Things machine for display to the outside is correct.

[0118] The first payment data can further include the settlement data at the payment serving end and the acquiring data at the Internet of Things machine serving end. In some embodiments, the settlement data at the payment serving end can be referred to as settlement data, and the acquiring data at the Internet of Things machine serving end can be referred to as acquiring data. The first payment data can include the settlement data and the acquiring data.

[0119] The performing consistency comparison between the first payment data and the second payment data can include: performing consistency comparison between the settlement data and the second payment data, and performing consistency comparison between the acquiring data and the settlement data.

[0120] Consistency comparison is performed between data stored at a plurality of ends, to further ensure accuracy of final payment result data.

[0121] A problem may occur at any node in a data transmission process, resulting in an error in a final payment result. Therefore, consistency comparison is performed between data at a plurality of ends, to help a developer quickly locate a node at which a problem occurs, so as to improve operation and maintenance efficiency.

[0122] The method provided in this disclosure can be deployed at any node in the payment system. For example, this solution can be deployed at the Internet of Things machine. Real-time consistency comparison can be implemented by deploying this solution at the Internet of Things machine. When inconsistency is found through comparison, the payment request with inconsistency can be intercepted in a timely manner, to ensure fund security of the user.

[0123] For another example, this solution can be deployed at the serving end. Specifically, this solution can be deployed at the Internet of Things machine serving end. Data consistency can be ensured from a source by deploying this solution at the serving end.

[0124] In some embodiments, this solution can alternatively be deployed at both the Internet of Things machine end and the serving end, to further ensure that the result page finally displayed to the user is consistent with the payment data stored at the serving end, that is, further ensure fund security of the user.

[0125] In some embodiments, this solution can alternatively be independently deployed on a verification platform. The payment process is monitored by using the verification platform, to ensure that what the user sees is what the user obtains.

[0126] The verification platform can be independent of the payment system. Therefore, in a manner of deploying the verification platform in the payment system, intrusion into the payment system can be avoided, making it simple to implement and easy to maintain.

[0127] The verification platform can monitor each transaction in real time. To improve processing efficiency of the verification platform, at a fixed time interval, all transactions in the time interval can be uniformly compared and processed. This manner of processing at a fixed time interval can also be referred to as automatic inspection. The time interval for inspection can be randomly selected based on a requirement. For example, inspection can be performed every 3 minutes.

[0128] FIG. 3 is a schematic flowchart of a payment security management method according to another embodiment of this disclosure. As shown in FIG. 3, a procedure of the payment security management method includes step S301 to step S312.

[0129] In step S301, a user makes a payment by using an Internet of Things machine. The Internet of Things machine can also be briefly referred to as a machine.

[0130] The Internet of Things machine can provide various payment channels for the user. For example, the Internet of Things machine can provide a face scanning or two-dimensional code scanning channel for the user.

[0131] The user can make a payment through face scanning or two-dimensional code scanning. For example, the user can submit a payment request to the Internet of Things machine through face scanning. The payment request can include a payment of 10 yuan to a merchant.

[0132] In step S302, the Internet of Things machine sends the payment request to a serving

end, to process the payment. The Internet of Things machine can communicate with the serving end through an Internet of Things, and send the payment request to the serving end.

[0133] In step S303, the serving end can process the payment request, and generate, based on a processing result, data required for a result page. In this embodiment, the result page is independently constructed by the serving end. Actually, the result page can be constructed by the serving end, can be constructed by the Internet of Things machine, or can be jointly constructed by the Internet of Things machine and the serving end. A specific manner of constructing the result page is not limited in this disclosure.

[0134] When the Internet of Things machine constructs the result page, two solutions are usually used: active polling and a solution in which unified payment sends a message to a device serving end.

[0135] Active polling includes that the Internet of Things machine actively requests data required for constructing the result page from the device serving end. After processing the payment request, unified payment also actively sends data to an Internet of Things machine serving end. After receiving the data, the Internet of Things machine serving end actively sends the data to the Internet of Things machine.

[0136] The result page is usually constructed based on a message that first arrives in the above-mentioned two solutions. In this embodiment, when the result page data is obtained, the result page data that first arrives at an Internet of Things machine end can be obtained by embedding a point at the Internet of Things machine end, and second payment data can be obtained based on the result page data.

[0137] In step S304, it is determined whether the payment succeeds.

[0138] When the payment fails, step S305 in which the serving end constructs payment failure information is performed. When the payment succeeds, step S306 in which the serving end constructs payment success information is performed.

[0139] In step S307, an information flow element for acquiring is obtained.

[0140] In step S308, a fund flow element for unified payment is obtained.

[0141] An information flow for acquiring and a fund flow for unified payment can be provided by a same serving end or by different serving ends. The information flow for acquiring and the fund flow for unified payment are usually provided by different serving ends. The information flow element for acquiring and the fund flow element for unified payment can uniformly generate

first payment data.

[0142] In step S309, an important fund flow/information flow element is compared.

[0143] There may also be a problem in a communication process between serving ends. For example, in the communication process between the serving ends, payment data may be tampered with. For another example, there may be a difference in data storage or construction logic between the serving ends, resulting in a difference in finally stored data.

[0144] Therefore, by performing consistency comparison between the first payment data and the second payment data, that is, by comparing the result page data, the information flow element for acquiring, and the fund flow element for unified payment, it can be found, in a timely manner, whether important data displayed on the result page is correct. The important data can include, for example, an important fund flow element and information flow element.

[0145] The fund flow element can include, for example, a user ID, a transaction number, a payment channel, a payment status, and a payment amount. The information flow element can include, for example, a payment method (for example, face scanning payment), device information of the Internet of Things machine (for example, a device SN code and a device MAC code).

[0146] In step S310, a comparison result is determined.

[0147] After the comparison fails, step S311 of giving an alarm and/or an emergency response is performed. The giving an alarm can include configuring alarm information, to alarm a developer when a same scenario occurs next time. The giving an alarm can alternatively include providing alarm information to a developer, so that the developer performs troubleshooting based on a log and the alarm information, and determine and resolve possible security vulnerabilities in the system.

[0148] After the comparison succeeds, step S312 of ending the procedure is performed.

[0149] With reference to FIG. 1 to FIG. 3, the foregoing describes in detail the method embodiments provided in this disclosure. With reference to FIG. 4 to FIG. 6, the following describes apparatus embodiments provided in this disclosure. It should be understood that the apparatus embodiments and the method embodiments correspond to each other. Therefore, for details not described in the apparatus embodiments, refer to the descriptions in the part of the method embodiments.

[0150] FIG. 4 is a schematic diagram of a structure of a payment security management apparatus according to an embodiment of this disclosure. The apparatus 400 can be applied to a

payment system. The payment system can include an Internet of Things machine and a serving end. The Internet of Things machine can be configured to send a payment request to the serving end. The serving end can be configured to respond to the payment request.

[0151] The apparatus 400 can include a first obtaining unit 410, a second obtaining unit 420, and a comparison unit 430.

[0152] The first obtaining unit 410 can be configured to obtain first payment data. The first payment data can be generated based on clearing data corresponding to the payment request.

[0153] The second obtaining unit 420 can be configured to obtain second payment data. The second payment data can be generated based on a result page corresponding to the payment request.

The result page can be used by the Internet of Things machine for display to the outside.

[0154] The comparison unit 430 can be configured to perform consistency comparison between the first payment data and the second payment data.

[0155] Optionally, in some embodiments, the serving end can include an Internet of Things machine serving end and a payment serving end. The clearing data can include acquiring data at the Internet of Things machine serving end and/or settlement data at the payment serving end.

[0156] Optionally, in some embodiments, the payment serving end can include unified payment.

[0157] Optionally, in some embodiments, the apparatus 400 can further include a storage unit. The storage unit can be configured to: after a comparison result is obtained, store the comparison result when the comparison result is "inconsistent".

[0158] Optionally, in some embodiments, the apparatus 400 can further include an interception unit. The interception unit can be configured to: after a comparison result is obtained, intercept the payment request when the comparison result is "inconsistent".

[0159] Optionally, in some embodiments, the first payment data and the second payment data can include an information flow and/or a fund flow corresponding to the payment request.

[0160] FIG. 5 is a schematic diagram of a payment system according to an embodiment of this disclosure. As shown in FIG. 5, the payment system can include an Internet of Things machine 510, a serving end 520, and a platform 530.

[0161] The Internet of Things machine 510 can be configured to send a payment request to the serving end.

[0162] The serving end 520 can be configured to process the payment request to generate

payment result data.

[0163] The platform 530 can be configured to perform the following operations: obtaining first payment data, where the first payment data is generated based on clearing data corresponding to the payment request; obtaining second payment data, where the second payment data is generated based on a result page corresponding to the payment request, and the result page is used by the Internet of Things machine for display to the outside; and performing consistency comparison between the first payment data and the second payment data, to obtain a comparison result.

[0164] The platform 530 can be implemented by hardware or software. A specific implementation form of the platform 530 is not limited in this disclosure.

[0165] The platform 530 can be independent of the Internet of Things machine 510 and the serving end 520. In some embodiments, the platform 530 can alternatively be deployed at the Internet of Things machine 510 and/or the serving end 520. A deployment location of the platform 530 is not limited in this disclosure.

[0166] FIG. 6 is a schematic diagram of a structure of a payment security management apparatus according to another embodiment of this disclosure. The apparatus 600 shown in FIG. 6 can be a platform that can perform the payment security management method provided in this disclosure. The apparatus 600 can be, for example, a computing device with a computing function. For example, the apparatus 600 can be a mobile terminal or a server. The apparatus 600 can include a memory 610 and a processor 620. The memory 610 can be configured to store executable code. The processor 620 can be configured to execute the executable code stored in the memory 610, to implement the steps in the methods described above. In some embodiments, the apparatus 600 can further include a network interface 630, and data exchange between the processor 620 and an external device can be implemented by using the network interface 630.

[0167] All or some of the above-mentioned embodiments can be implemented by using software, hardware, firmware, or any other combination. When software is used for implementation, all or some of the above-mentioned embodiments can be implemented in a form of a computer program product. The computer program product includes one or more computer program instructions. When the computer program instructions are loaded and executed on a computer, all or some of the procedures or functions according to the embodiments of this disclosure are generated. The computer can be a general-purpose computer, a dedicated computer, a computer network, or another programmable apparatus. The computer instructions can be stored

in a computer-readable storage medium, or can be transmitted from a computer-readable storage medium to another computer-readable storage medium. For example, the computer instructions can be transmitted from a website, computer, server, or data center to another website, computer, server, or data center in a wired (for example, a coaxial cable, an optical fiber, or a digital subscriber line (DSL)) or wireless (for example, infrared, radio, or microwave) manner. The computer-readable storage medium can be any usable medium accessible by the computer, or a data storage device, for example, a server or a data center, into which one or more usable media are integrated. The usable medium can be a magnetic medium (for example, a floppy disk, a hard disk, or a magnetic tape), an optical medium (for example, a digital video disc (DVD)), a semiconductor medium (for example, a solid state disk (SSD)), or the like.

[0168] A person of ordinary skill in the art can be aware that the example units, algorithms, and steps described with reference to the embodiments of this disclosure can be implemented by electronic hardware or a combination of computer software and electronic hardware. Whether the functions are performed by hardware or software depends on particular applications and design constraints of the technical solutions. A person skilled in the art can use different methods to implement the described functions for each particular application, but it should not be considered that the implementation goes beyond the scope of this disclosure.

[0169] In the several embodiments provided in this disclosure, it should be understood that the disclosed system, apparatus, and method can be implemented in other manners. For example, the apparatus embodiments described above are merely examples. For example, division into the units is merely logical function division and may be other division in an actual implementation. For example, a plurality of units or components can be combined or integrated into another system, or some features may be ignored or not performed. In addition, the displayed or discussed mutual couplings or direct couplings or communication connections can be implemented by using some interfaces. The indirect couplings or communication connections between the apparatuses or units can be implemented in electronic, mechanical, or other forms.

[0170] The units described as separate parts may or may not be physically separate, and parts displayed as units may or may not be physical units, that is, may be located at one location, or may be distributed on a plurality of network units. Some or all of the units can be selected based on actual requirements to achieve the objectives of the solutions in the embodiments.

[0171] In addition, functional units in the embodiments of this disclosure can be integrated

into one processing unit, each of the units can exist alone physically, or two or more units can be integrated into one unit.

[0172] The above-mentioned descriptions are merely specific implementations of this disclosure, but the protection scope of this disclosure is not limited thereto. Any variation or replacement readily figured out by a person skilled in the art within the technical scope disclosed
5 in this disclosure shall fall within the protection scope of this disclosure. Therefore, the protection scope of this disclosure shall be subject to the protection scope of the claims.

CLAIMS

What is claimed is:

1. A payment security management method, applied to a payment system, wherein the payment system comprises an Internet of Things machine and a serving end, the Internet of Things machine is configured to send a payment request to the serving end, the serving end is configured to respond to the payment request, and the method comprises:
 - obtaining first payment data, wherein the first payment data is generated based on clearing data corresponding to the payment request;
 - obtaining second payment data, wherein the second payment data is generated based on a result page corresponding to the payment request, and the result page is used by the Internet of Things machine for display to the outside; and
 - performing consistency comparison between the first payment data and the second payment data, to obtain a comparison result.
2. The method according to claim 1, wherein the serving end comprises an Internet of Things machine serving end and a payment serving end, and the clearing data comprises acquiring data at the Internet of Things machine serving end and/or settlement data at the payment serving end.
3. The method according to claim 2, wherein the payment serving end comprises unified payment.
4. The method according to claim 1, wherein after the obtaining a comparison result, the method further comprises:
 - storing the comparison result when the comparison result is "inconsistent".
5. The method according to claim 1, wherein after the obtaining a comparison result, the method further comprises:
 - intercepting the payment request when the comparison result is "inconsistent".
6. The method according to claim 1, wherein the first payment data and the second payment data comprise information flow data and/or fund flow data corresponding to the payment request.
7. A payment security management apparatus, applied to a payment system, wherein the payment system comprises an Internet of Things machine and a serving end, the Internet of Things machine is configured to send a payment request to the serving end, the serving end is configured to respond to the payment request, and the apparatus comprises:

a first obtaining unit, configured to obtain first payment data, wherein the first payment data is generated based on clearing data corresponding to the payment request;

a second obtaining unit, configured to obtain second payment data, wherein the second payment data is generated based on a result page corresponding to the payment request, and the
5 result page is used by the Internet of Things machine for display to the outside; and

a comparison unit, configured to perform consistency comparison between the first payment data and the second payment data, to obtain a comparison result.

8. The apparatus according to claim 7, wherein the serving end comprises an Internet of Things machine serving end and a payment serving end, and the clearing data comprises acquiring
10 data at the Internet of Things machine serving end and/or settlement data at the payment serving end.

9. The apparatus according to claim 8, wherein the payment serving end comprises unified payment.

10. The apparatus according to claim 7, further comprising:

15 a storage unit, configured to: after the comparison result is obtained, store the comparison result when the comparison result is "inconsistent".

11. The apparatus according to claim 7, further comprising:

an interception unit, configured to: after the comparison result is obtained, intercept the payment request when the comparison result is "inconsistent".

20 12. The apparatus according to claim 7, wherein the first payment data and the second payment data comprise an information flow and/or a fund flow data corresponding to the payment request.

13. A payment system, comprising:

an Internet of Things machine, configured to send a payment request to a serving end;

25 the serving end, configured to process the payment request to generate payment result data;
and

a platform, configured to perform the following operations:

obtaining first payment data, wherein the first payment data is generated based on clearing data corresponding to the payment request;

30 obtaining second payment data, wherein the second payment data is generated based on a result page corresponding to the payment request, and the result page is used by the Internet of

Things machine for display to the outside; and

performing consistency comparison between the first payment data and the second payment data, to obtain a comparison result.

14. A payment security management apparatus, comprising:

5 a memory, configured to store instructions; and

a processor, configured to execute the instructions stored in the memory, to perform the method according to any one of claims 1 to 6.