Technical Disclosure Commons

Defensive Publications Series

December 2021

SYSTEM AND METHOD FOR MONITORING FRAUDELENT TRANSACTIONS AT MERCHANT LEVEL IN REAL TIME PAYMENT

Ila Malde

Juharasha Shaik

Aditi Khare

Durga Kala

Kenny Tsai

See next page for additional authors

Follow this and additional works at: https://www.tdcommons.org/dpubs_series

Recommended Citation

Malde, Ila; Shaik, Juharasha; Khare, Aditi; Kala, Durga; Tsai, Kenny; Miryala, Ram; Ranjan, Rajiv; Chakraborty, Santanu; Li, Xuepeng; Mahadev, Anup; Masharov, Andrey; Paudel, Mohan; Chowdhury, Debabrata; Kankatala, Ramya; Mahanta, Motilal; Pandya, Chintan; and Srinivas, Manasa, "SYSTEM AND METHOD FOR MONITORING FRAUDELENT TRANSACTIONS AT MERCHANT LEVEL IN REAL TIME PAYMENT", Technical Disclosure Commons, (December 03, 2021)
https://www.tdcommons.org/dpubs_series/4761

This work is licensed under a Creative Commons Attribution 4.0 License.
This Article is brought to you for free and open access by Technical Disclosure Commons. It has been accepted for inclusion in Defensive Publications Series by an authorized administrator of Technical Disclosure Commons.

Inventor(s)
Ila Malde, Juharasha Shaik, Aditi Khare, Durga Kala, Kenny Tsai, Ram Miryala, Rajiv Ranjan, Santanu Chakraborty, Xuepeng Li, Anup Mahadev, Andrey Masharov, Mohan Paudel, Debabrata Chowdhury, Ramya Kankatala, Motilal Mahanta, Chintan Pandya, and Manasa Srinivas

This article is available at Technical Disclosure Commons: https://www.tdcommons.org/dpubs_series/4761

SYSTEM AND METHOD FOR MONITORING FRAUDELENT TRANSACTIONS AT MERCHANT LEVEL IN REAL TIME PAYMENT

TECHNICAL FIELD

[001] The present disclosure relates generally to financial transactions. More particularly, the present disclosure relates to monitoring fraudulent transactions during the transaction, and more particularly on monitoring and avoiding fraud at the merchant level.

BACKGROUND

[002] In today's marketplace making online payments for buying goods and services are popular. While making transactions, customers need to know their account information will be protected, and merchant needs tools to confirm the validity of transactions.

[003] In the payments industry, without the knowledge of real cardholder, the card details are used illegally. A stolen credit card or card number is usually the cause of a fraudulent transactions. Fraud detection is difficult, if stolen payment details are accepted by the merchant and the merchant and/ or the real customer may not know until a significant time after the purchased items by the fraudster. Thus, fraudulent transactions need to be identified. The fraudulent transactions also lead to loss of revenue to the merchant in the form of transaction charges.

[004] Thus, what is needed is a secure, efficient and fast systems to monitor fraudulent transaction which helps the customers to protect their card details and helps the merchants to detect fraud transactions and prevent them to rely on other third party system for monitoring fraud. The information disclosed in this background of the disclosure section is only for

enhancement of understanding of the general background of the invention and should not be taken as an acknowledgement or any form of suggestion that this information forms the prior art already known to a person skilled in the art.

SUMMARY

[005] The present invention aims at detecting fraudulent transactions at marketplace with the help of intelligent rules and risk manager to confirm the validity of transactions and to achieve the highest payment success rate while reducing transaction processing costs on the blocked fraudulent transactions. In one embodiment, a computer-implemented method of authorising transactions is proposed. The method comprises providing, a direct access of issuer authorization rules engine to the merchant to evaluate and block card payment transaction from potential fraud at checkout. Further, enabling a secure connection to a Risk Manager (RM) for providing an access to the intelligent rules. The method further comprises empowering the merchant to not forward the fraudulent transaction onto the acquirer for further processing. The method also allows the merchants to define their own rules to reduce fraudulent transaction at the merchant level or POS terminal (104). The method further comprises generating rules using artificial intelligence and based on the merchant performance insights or merchant data points. Thereafter, integrating RM with merchant server (102) and providing tools to confirm the validity of transaction.

[006] The foregoing summary is illustrative only and is not intended to be in any way limiting. In addition to the illustrative aspects, embodiments, and features described above, further aspects, embodiments, and features will become apparent by reference to the drawings and the following detailed description.

BRIEF DESCRIPTION OF THE DRAWINGS

[007] The example embodiment(s) of the present invention are illustrated by way of example, and not in way by limitation, in the figures of the accompanying drawings and in which like reference numerals refer to similar elements and in which:

[008] Figure 1 depicts a payment transaction environment, in accordance with an embodiment of the present disclosure;

[009] Figure 2 illustrates an exemplary flow of method to monitor and avoid fraudulent transactions at merchant level in real time payment, in accordance with an embodiment of the present disclosure;

[0010] Figure 3 shows a block diagram of a computer apparatus in accordance with an embodiment;

[0011] It should be appreciated by those skilled in the art that any block diagrams herein represent conceptual views of illustrative systems embodying the principles of the present subject matter. Similarly, it will be appreciated that any flow charts, flow diagrams, state transition diagrams, pseudo code, and the like represent various processes which may be substantially represented in computer readable medium and executed by a computer or processor, whether or not such computer or processor is explicitly shown. While each of the figures illustrates a particular embodiment for purposes of illustrating a clear example, other embodiments may omit, add to, reorder, and/or modify any of the elements shown in the figures.

DETAILED DESCRIPTION

[0012] In the present document, the word "exemplary" is used herein to mean "serving as an example, instance, or illustration." Any embodiment or implementation of the present subject matter described herein as "exemplary" is not necessarily to be construed as preferred or advantageous over other embodiments.

[0013] While the disclosure is susceptible to various modifications and alternative forms, specific embodiment thereof has been shown by way of example in the drawings and will be described in detail below. It should be understood, however that it is not intended to limit the disclosure to the particular forms disclosed, but on the contrary, the disclosure is to cover all modifications, equivalents, and alternative falling within the scope of the disclosure.

[0014] The terms “comprises”, “comprising”, or any other variations thereof, are intended to cover a non-exclusive inclusion, such that a setup, device or method that comprises a list of components or steps does not include only those components or steps but may include other components or steps not expressly listed or inherent to such setup or device or method. In other words, one or more elements in a system or apparatus proceeded by “comprises… a” does not, without more constraints, preclude the existence of other elements or additional elements in the system or apparatus.

[0015] Point of Sales (POS) system is a machine introduced at Merchant Establishments which empowers the enables the merchants to accept payments through payment cards (credit cards, debit cards, gift cards etc.). The establishment of POS machine at a vendor outlet will reduce cash handling and will improve business income for merchants through expanded spending choice. It is a strategy for issue free looking for customers as they don’t need to carry cash with them.

[0016] Transactions in which a consumer payment device is presented to a merchant or accessed by a point-of-sale terminal are termed "card present" transactions since the payment device is in the same physical location as the merchant or terminal.

[0017] In addition to card present transactions, a consumer may also initiate a transaction in a situation in which the payment device is not in the same physical location as the merchant or terminal, and instead the relevant data is provided over a communications network to the merchant (termed a "card not present" transaction). For example, a card not present transaction involving the purchase of a product or service may be initiated by a consumer by providing payment data from a remote location to a merchant over a network such as the Internet. Transactions of this type are typically initiated using a computing device such as a personal computer or laptop computer. Card not present transactions may also be initiated or performed using a mobile payment device such as a mobile phone, in which case communication with a merchant or data processing system may occur over a cellular or wireless network. Thus, payment information for a transaction may be provided using a payment device and point of sale terminal or may be provided to a merchant using a remotely located payment device, among other methods.

[0018] Existing fraud detection systems contain fraud detection rules that help in evaluate transactions and guide merchants in deciding if a particular transaction is valid or fraud using different algorithms. However, fraud detection rules vary as each industry and also each merchant is different. In Today’s market marketplace making a transaction must be easy, safe and fast which helps both customers and merchants.

[0019] Today Merchant is reliant on many other systems to detect fraud on their behalf. Merchants need advance solutions that can provide full context of each transaction, analyse the surrounding ecosystem, continuously monitor card holder data.

[0020] Fraud on Card Not Present (CNP) or Point of Sales (POS) at any Merchant site is highly vulnerable as that is the first step of the payment transaction processing lifecycle, and least protected.

[0021] Generally, an issuing bank provides debit/credit card to the card holder where card can be used to shop online or at POS terminals. With each purchase payment request is sent to acquiring bank via payment gateway. The acquiring bank then sends the request through the relevant card scheme back to the issuing bank for authorization. When authorized and the payment is successful, the merchant can deliver the goods and services. Merchant account is needed because it enables merchant to legally accept and process payments through all payment methods. Also, it provides safe payment options to their customers, protect the sensitive data and protect themselves from fraudulent transactions and chargebacks. Merchant account holders are required to abide by the rules and regulations set by the card schemes (network server).

[0022] Embodiments of the present disclosure relate to methods and systems for monitoring and detecting the fraud transactions to prevent the huge revenue losses at the merchant level and to provide secure, fast and easy payment transactions to take place with the usage of artificial intelligence and risk manager.

[0023] Figure 1 illustrates a typical payment environment 100. The environment (100) comprises a merchant, offering product or services to the customers, the customer, also called cardholder wants to access products and services that the merchant is selling, and initiates transaction. An issuer bank is the customer bank that issues the cardholder's credit or debit card on behalf of the card schemes. An acquirer server (101) maintains the merchant's bank account and all the transaction details. The acquiring server (101), connected to a network server (107) passes the merchant's transactions to an issuer server (106) to receive payment. The acquirer server (101) is further connected to merchant server (102) to access and forward all the transaction details by defining one or more rules. The merchant server (102) is connected to the network server (107) and handles purchases and credit card transactions initiated by customers. The merchant server (102) is further connected to a Point of Sales (POS) system (103) and ensures secure transmission of payments of clients that provides service by connecting with cooperative banks. The POS system (103) may be connected to a POS terminal (104) that processes payments for goods and services from customers and keeps track of sale. The POS terminal (104) may include a card reader that lets customers securely pay by credit card/debit card while in-store, whether that's through a contactless payment like wallet payment/magnetic stripe card or a chip card. The network server (105) is connected to the issuer server (106) and provides a payment gateway to access and transfer transactions between acquirer server (101) and issuer server (106).

[0024] Reference is now made to Figure 2. The following method describes the steps performed by the merchant server (102). Figure 2 is a flowchart describing a method for fraud detection in payment transactions at merchant level, in accordance with an embodiment of the present disclosure.

[0025] As illustrated in Figure 2, the method 200 may comprise one or more steps. The method 200 may be described in the general context of computer executable instructions. Generally, computer executable instructions can include routines, programs, objects, components, data structures, procedures, modules, and functions, which perform particular functions or implement particular abstract data types.

[0026] The order in which the method (200) is described is not intended to be construed as a limitation, and any number of the described method blocks can be combined in any order to implement the method. Additionally, individual blocks may be deleted from the methods without departing from the scope of the subject matter described herein. Furthermore, the method can be implemented in any suitable hardware, software, firmware, or combination thereof.

[0027] The following steps are performed after the merchant server (102) direct access to the powerful issuer authorization rules engine to evaluate and block card payment transaction in real-time from potential fraud at checkout and transfer information to the acquirer server (101).

[0028] At step 201, providing direct access to merchant server (102) to access issuer authorization rules engine hosted in the issuer server (106) to evaluate and block card payment transaction in real-time from potential fraud at checkout wherein, authorization rules engine includes pre-determined condition to be satisfied by the issuer card to evaluate if card details are fraud and block card transaction. The rules may define conditions that needs to be met for a transaction to be processed. The rules may be defined by a domain expert or a computer.

[0029] At step 202, enabling secure connection to the Risk Manager (RM) to access the intelligent rules wherein, RM comprises a complete set of fraud and risk management tools that can be accessed through online and evaluated risk management methods during payment by accessing the card details. The RM may be an application (web application or a phone application) configured by the network server (105) to enable the merchant to identify fraudulent transactions. The RM may include the rules defined by the issuer server (102). The RM may also include rules defined by the network server (105). Also, provision may be provided for the merchant to define the rules. The RM may store fraudulent transactions flagged by the issuer server (106), the merchant server (102). The RM may be accessed by the merchant server (102) using an API call. The RM may also be accessed via web browser. The RM may be hosted in the network server (105).

[0030] At step 203, empowering the merchant server (102) by real-time data not to forward the fraudulent transaction onto the acquirer server (101) for further processing and saving the transaction processing fees as eliminating back-office overheads on failed payments. The merchant server (102) may be provided an API to access the RM when a transaction occurs. The merchant server (102) can determine if the conditions of the transactions meet the rules provided in the RM. When the conditions do not match the rules, the transaction can be flagged as a fraudulent transaction. For example, when the merchant server (102) detects an initiation of a transaction, but the card is not detected by the POS terminal (104), such a transaction can be flagged as a fraudulent transaction. For example, when fraudster tries to purchase goods and services using the stolen card details and the merchant server (102) detects an initiation of transaction, but when the card details are not authorized by the card holder to process the transaction as the conditions do not match the rules defined by the issuer, such a transaction can be flagged as a fraudulent transaction.

[0031] At step 204, enabling the merchants to define their own rules to reduce fraudulent transactions at the merchant level or on POS terminals wherein the payment card details should satisfy all the protocols set by merchant in order to proceed with transaction. The merchant may be provided to define their rules based on the different transactions monitored by the merchant server (102). The merchant generated rules can be added to the RM.

[0032] At step 205, generating smarter rules using artificial intelligence and based on the merchant performance insights or merchant data points wherein, the intelligent rules will provide protection against potential card payment fraudulent transaction that could slip through the "floor limit" rules set by merchant. AI models may be used to detect fraudulent transactions. Big data is useful in training the AI models. For example, the merchant server (102) can provide a plurality of transaction data to an AI model (supervised or unsupervised). The AI model may classify the transactions into normal transactions and fraudulent transactions. Further, the trained AI model can be used in real-time to detect fraudulent transactions and flag the transaction. The network server (105) may also implement the AI model to detect the fraudulent transactions and update the RM with new rules. The use of the AI model constantly improves the RM and reduces processing fraudulent transactions. This decreases the overhead on the merchant.

[0033] At step 206, integrating the RM with merchant server (102) and providing tools to confirm the validity of transaction which helps in the highest payment success rate while reducing transaction processing costs on the blocked fraudulent transactions. Risk Manager may be a web-based suite of tools providing issuers with control and flexibility to manage to their risk strategies and risk tolerance. As the risk manager (RM) contains one or more risk and

fraud detection tools that can be accessed through online to detect fraudulent transactions and confirms the validity of transaction. With RM, merchant server (102) can run rules before authorization to help reduce costs, capture revenue, and over time, help improve authorization rates by filtering out risky transactions and achieving high success rate in plurality of transactions by connection RM with merchant server (102). For example, when merchant server (102) accepts the card of issuer to initiate transaction. Firstly, RM verifies the card/account details with the rules defined by the issuer server (106) with all risk management tools contained in it and verifies if the transaction is “valid” or “fraudulent” and sends the message to merchant server (102).

[0034] Figure 3 illustrates a block diagram of an exemplary computer system (300) for implementing embodiments consistent with the present disclosure. In an embodiment, the computer system (300) is used to implement the method for authorising transactions in the platform (300). The computer system (300) may comprise a central processing unit (“CPU” or “processor”) (302). The processor (302) may comprise at least one data processor for executing program components for dynamic resource allocation at run time. The processor (302) may include specialized processing units such as integrated system (bus) controllers, memory management control units, floating point units, graphics processing units, digital signal processing units, etc.

[0035] The processor (302) may be disposed in communication with one or more input/output (I/O) devices (not shown) via I/O interface (301). The I/O interface (301) may employ communication protocols/methods such as, without limitation, audio, analog, digital, monoaural, RCA, stereo, IEEE-1394, serial bus, universal serial bus (USB), infrared, PS/2, BNC, coaxial, component, composite, digital visual interface (DVI), high-definition

multimedia interface (HDMI), RF antennas, S-Video, VGA, IEEE 802.n /b/g/n/x, Bluetooth, cellular (e.g., code-division multiple access (CDMA), high-speed packet access (HSPA+), global system for mobile communications (GSM), long-term evolution (LTE), WiMax, or the like), etc.

[0036] Using the I/O interface (301), the computer system (300) may communicate with one or more I/O devices. For example, the input device (310) may be an antenna, keyboard, mouse, joystick, (infrared) remote control, camera, card reader, fax machine, dongle, biometric reader, microphone, touch screen, touchpad, trackball, stylus, scanner, storage device, transceiver, video device/source, etc. The output device 311 may be a printer, fax machine, video display (e.g., cathode ray tube (CRT), liquid crystal display (LCD), light-emitting diode (LED), plasma, Plasma display panel (PDP), Organic light-emitting diode display (OLED) or the like), audio speaker, etc.

[0037] In some embodiments, the computer system (300) is connected to the service operator through a communication network (309). The processor (302) may be disposed in communication with the communication network (309) via a network interface (303). The network interface (303) may communicate with the communication network (309). The network interface (303) may employ connection protocols including, without limitation, direct connect, Ethernet (e.g., twisted pair 10/100/1000 Base T), transmission control protocol/Internet protocol (TCP/IP), token ring, IEEE 802.11a/b/g/n/x, etc. The communication network (309) may include, without limitation, a direct interconnection, e-commerce network, a peer to peer (P2P) network, local area network (LAN), wide area network (WAN), wireless network (e.g., using Wireless Application Protocol), the Internet, Wi-Fi, etc.

Using the network interface (303) and the communication network (309), the computer system 400 may communicate with the one or more service operators.

[0038] In some embodiments, the processor (302) may be disposed in communication with a memory (305) (e.g., RAM, ROM, etc) via a storage interface (304). The storage interface (304) may connect to memory (305) including, without limitation, memory drives, removable disc drives, etc., employing connection protocols such as serial advanced technology attachment (SATA), Integrated Drive Electronics (IDE), IEEE-1394, Universal Serial Bus (USB), fibre channel, Small Computer Systems Interface (SCSI), etc. The memory drives may further include a drum, magnetic disc drive, magneto-optical drive, optical drive, Redundant Array of Independent Discs (RAID), solid-state memory devices, solid-state drives, etc.

[0039] The memory (305) may store a collection of program or database components, including, without limitation, user interface (306), an operating system (307), web server (308) etc. In some embodiments, computer system (300) may store user/application data (306), such as the data, variables, records, etc. as described in this disclosure. Such databases may be implemented as fault-tolerant, relational, scalable, secure databases such as Oracle or Sybase.

[0040] The operating system (307) may facilitate resource management and operation of the computer system (300). Examples of operating systems include, without limitation, Apple Macintosh OS X, Unix, Unix-like system distributions (e.g., Berkeley Software Distribution (BSD), FreeBSD, NetBSD, OpenBSD, etc.), Linux distributions (e.g., Red Hat, Ubuntu, Kubuntu, etc.), IBM OS/2, Microsoft Windows (XP, Vista/7/8, 10 etc.), Apple iOS, Google Android, Blackberry OS, or the like.

[0041] In some embodiments, the computer system (300) may implement a web browser (308) stored program component. The web browser (308) may be a hypertext viewing application, such as Microsoft Internet Explorer, Google Chrome, Mozilla Firefox, Apple Safari, etc. Secure web browsing may be provided using Secure Hypertext Transport Protocol (HTTPS), Secure Sockets Layer (SSL), Transport Layer Security (TLS), etc. Web browsers (308) may utilize facilities such as AJAX, DHTML, Adobe Flash, JavaScript, Java, Application Programming Interfaces (APIs), etc. In some embodiments, the computer system (300) may implement a mail server stored program component. The mail server may be an Internet mail server such as Microsoft Exchange, or the like. The mail server may utilize facilities such as ASP, ActiveX, ANSI C++/C#, Microsoft .NET, CGI scripts, Java, JavaScript, PERL, PHP, Python, WebObjects, etc. The mail server may utilize communication protocols such as Internet Message Access Protocol (IMAP), Messaging Application Programming Interface (MAPI), Microsoft Exchange, Post Office Protocol (POP), Simple Mail Transfer Protocol (SMTP), or the like. In some embodiments, the computer system (300) may implement a mail client stored program component. The mail client may be a mail viewing application, such as Apple Mail, Microsoft Entourage, Microsoft Outlook, Mozilla Thunderbird, etc.

[0042] In an embodiment, the computer system (300) is a directory server providing services for facilitating transactions between a merchant associated with an acquirer system, and an issuer system. In an embodiment, the computer system (300) is connected to the entities comprising the merchant, acquirer system, issuer system.

[0043] The terms "an embodiment", "embodiment", "embodiments", "the embodiment", "the embodiments", "one or more embodiments", "some embodiments", and "one embodiment"

mean "one or more (but not all) embodiments of the invention(s)" unless expressly specified otherwise.

[0044] The terms "including", "comprising", “having” and variations thereof mean "including but not limited to", unless expressly specified otherwise.

[0045] The enumerated listing of items does not imply that any or all of the items are mutually exclusive, unless expressly specified otherwise. The terms "a", "an" and "the" mean "one or more", unless expressly specified otherwise.

[0046] A description of an embodiment with several components in communication with each other does not imply that all such components are required. On the contrary a variety of optional components are described to illustrate the wide variety of possible embodiments of the invention.

[0047] When a single device or article is described herein, it will be readily apparent that more than one device/article (whether or not they cooperate) may be used in place of a single device/article. Similarly, where more than one device or article is described herein (whether or not they cooperate), it will be readily apparent that a single device/article may be used in place of the more than one device or article or a different number of devices/articles may be used instead of the shown number of devices or programs. The functionality and/or the features of a device may be alternatively embodied by one or more other devices which are not explicitly described as having such functionality/features. Thus, other embodiments of the invention need not include the device itself.

[0048] Finally, the language used in the specification has been principally selected for readability and instructional purposes, and it may not have been selected to delineate or circumscribe the inventive subject matter. It is therefore intended that the scope of the invention be limited not by this detailed description, but rather by any claims that issue on an application based here on. Accordingly, the disclosure of the embodiments of the invention is intended to be illustrative, but not limiting, of the scope of the invention, which is set forth in the following claims.

[0049] While various aspects and embodiments have been disclosed herein, other aspects and embodiments will be apparent to those skilled in the art. The various aspects and embodiments disclosed herein are for purposes of illustration and are not intended to be limiting, with the true scope and spirit being indicated by the following claims.

SYSTEM AND METHOD FOR MONITORING FRAUDELENT TRANSACTIONS AT MERCHANT LEVEL IN REAL TIME PAYMENT

ABSTRACT

Disclosed herein is a method and system providing Merchants direct access to the powerful issuer authorization rules engine to evaluate and block card payment transaction in real-time from potential fraud at checkout. The access to the intelligent rules can be made by enabling a secure connection to the Risk Manager (RM). The real-time data will empower the Merchant to not forward the fraudulent transaction onto the acquirer for further processing, saving the transaction processing fees as eliminating back-office overheads on failed payments.

Fig. 2

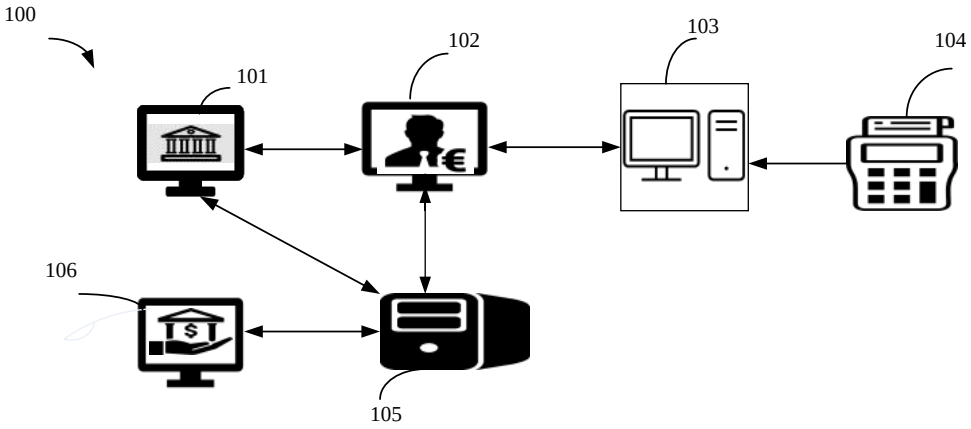

Figure 1

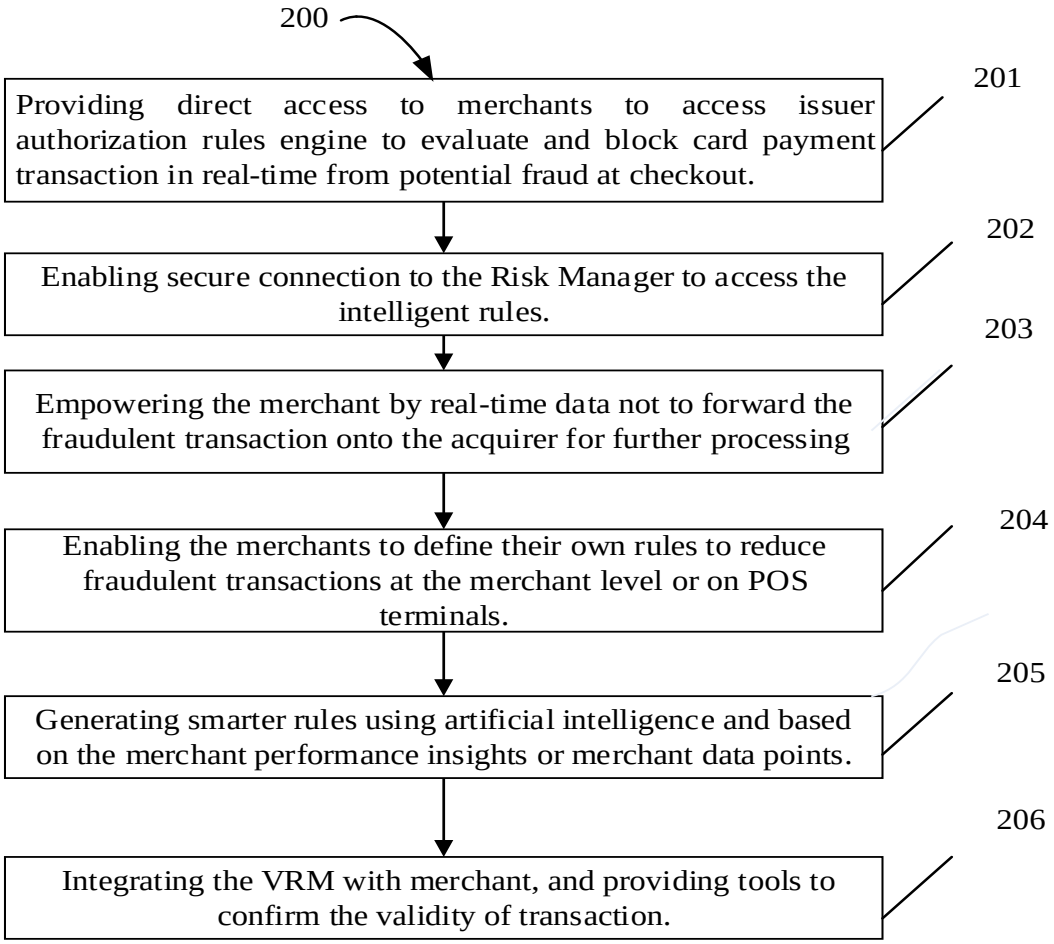
200
Providing direct access to merchants to access issuer authorization rules engine to evaluate and block card payment transaction in real-time from potential fraud at checkout.
201
Enabling secure connection to the Risk Manager to access the intelligent rules.
202
Empowering the merchant by real-time data not to forward the fraudulent transaction onto the acquirer for further processing
203
Enabling the merchants to define their own rules to reduce fraudulent transactions at the merchant level or on POS terminals.
204
Generating smarter rules using artificial intelligence and based on the merchant performance insights or merchant data points.
205
Integrating the VRM with merchant, and providing tools to confirm the validity of transaction.
206

Figure 2

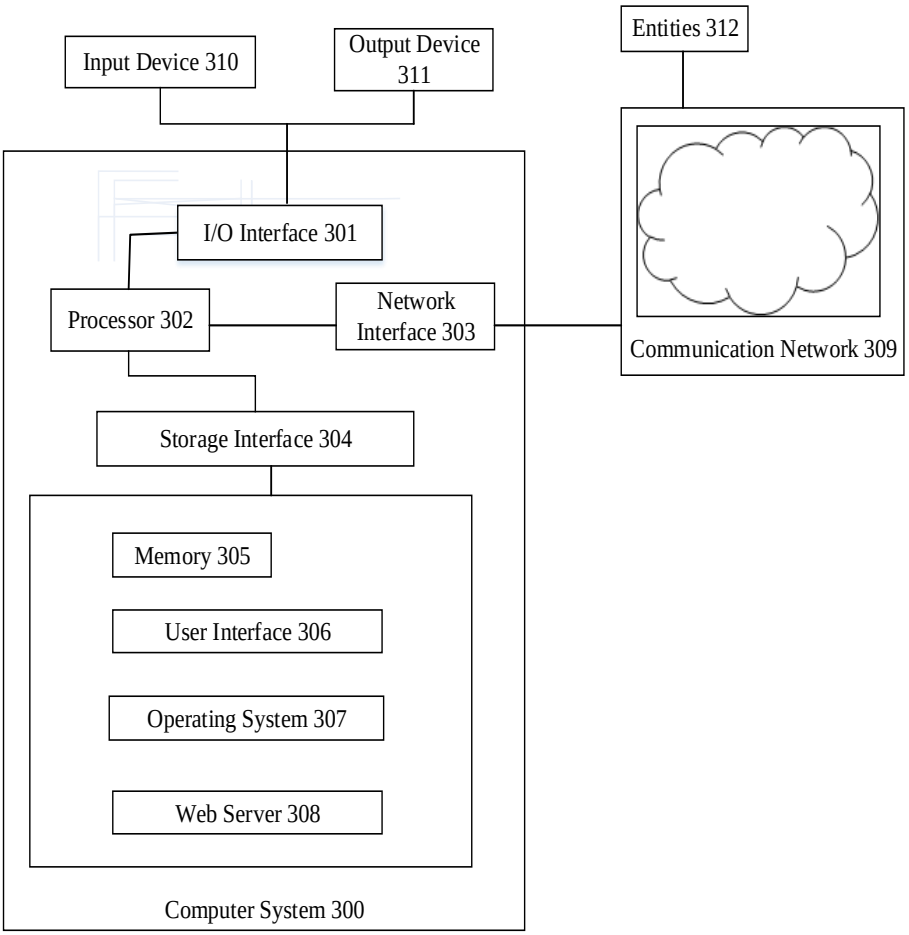
Entities 312
Input Device 310
Output Device 311
I/O Interface 301
Processor 302
Network Interface 303
Communication Network 309
Storage Interface 304
Memory 305
User Interface 306
Operating System 307
Web Server 308
Computer System 300

Figure 3