US 20190147450A1

(19) United States

(12) Patent Application Publication (10) Pub. No.: US 2019/0147450 A1

Bharghavan et al. (43) Pub. Date: May 16, 2019

(54) **REAL-TIME ENRICHMENT OF RAW MERCHANT DATA FROM ISO TRANSACTIONS ON DATA COMMUNICATION NETWORKS FOR PREVENTING FALSE DECLINES IN FRAUD PREVENTION SYSTEMS**

(71) Applicant: **Ondot System**, San Jose, CA (US)

(72) Inventors: **Vaduvur Bharghavan**, MORGAN HILL, CA (US); **Sung-Wook Han**, Sunnyvale, CA (US); **Zhiqiang Zhang**, San Ramon, CA (US)

(21) Appl. No.: **16/227,560**

(22) Filed: **Dec. 20, 2018**

Related U.S. Application Data

(63) Continuation-in-part of application No. 13/527,544, filed on Jun. 19, 2012, Continuation-in-part of application No. 14/058,229, filed on Oct. 19, 2013.

Publication Classification

(51) **Int. Cl.**

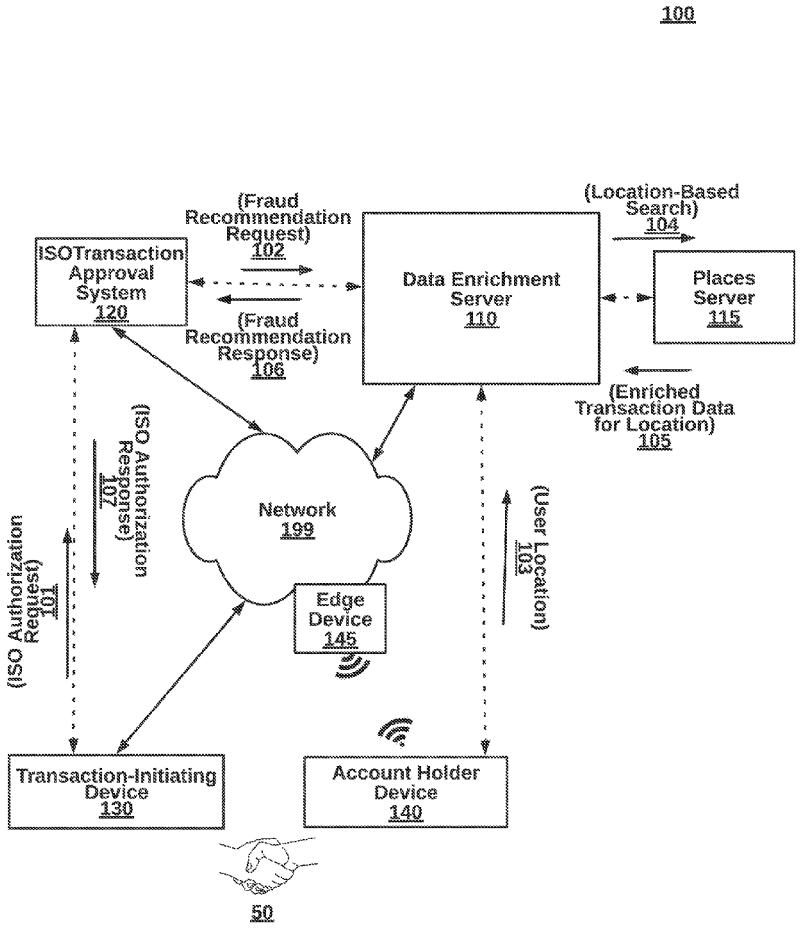
G06Q 20/40	(2006.01)
G06Q 20/32	(2006.01)
G06Q 20/38	(2006.01)

(52) **U.S. Cl.**

CPC ***G06Q 20/4016*** (2013.01); ***G06Q 20/388*** (2013.01); ***G06Q 20/3226*** (2013.01); ***G06Q 20/3224*** (2013.01)

(57) **ABSTRACT**

Raw merchant data of real-time ISO transactions is enriched with normalized merchant data, including a normalized merchant name, a normalized merchant location, by transmitting the raw merchant data to an external resource and receiving the normalized raw merchant data from the external resource. An authorization request from a real-time ISO transaction concerning a specific mobile user can be initiated by a specific merchant device at a merchant location. A user location is obtained and utilized to identify enriched merchant data. It is the enriched merchant data that is used for deciding whether to approve or deny a transaction with more accuracy.



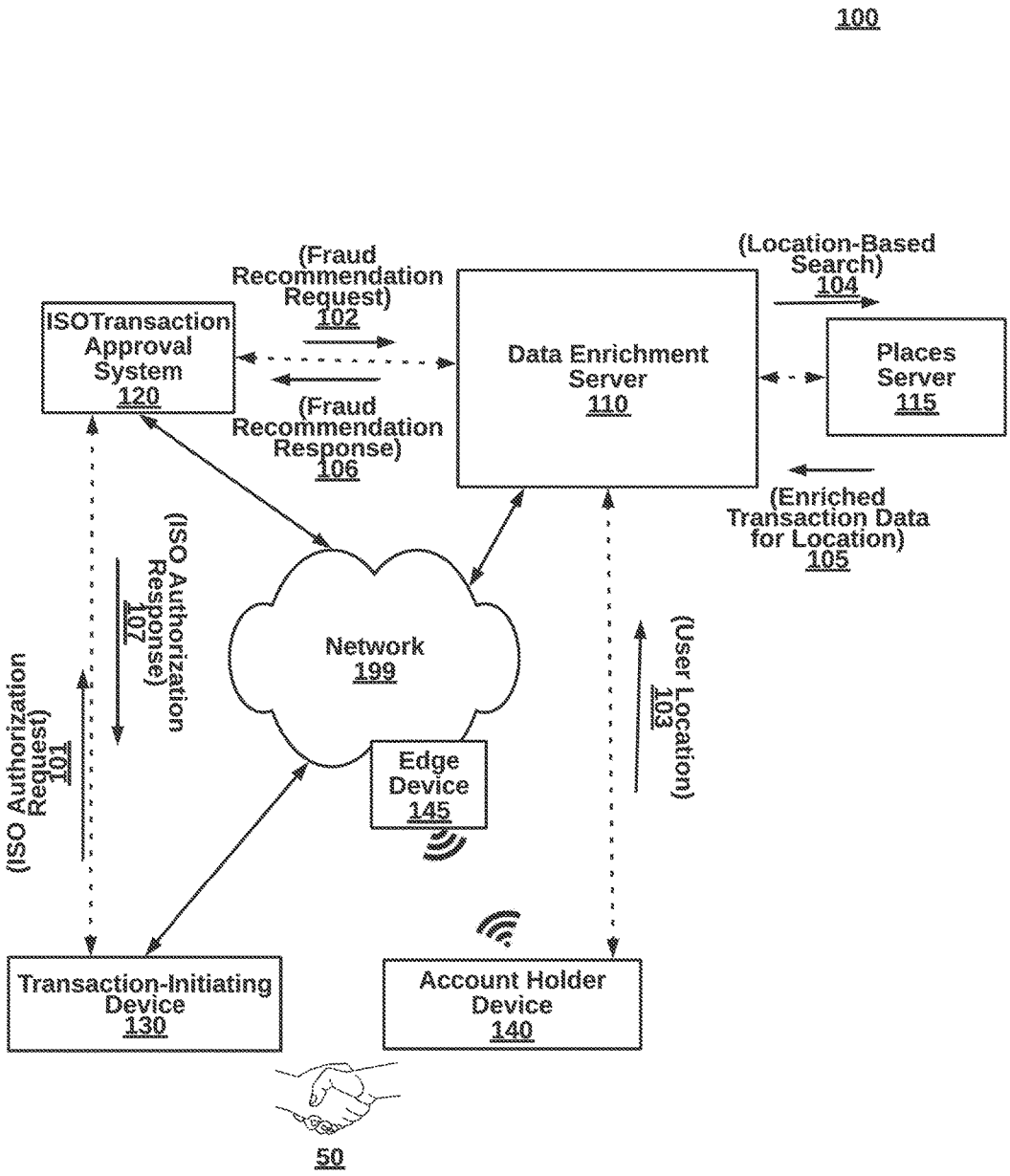

100
(Fraud Recommendation Request) 102
(Location-Based Search) 104
ISOTransaction Approval System 120
Data Enrichment Server 110
Places Server 115
(Fraud Recommendation Response) 106
(Enriched Transaction Data for Location) 105
(ISO Authorization Response) 107
Network 199
(ISO Authorization Request) 101
(User Location) 103
Edge Device 145
Transaction-Initiating Device 130
Account Holder Device 140
50

FIG. 1

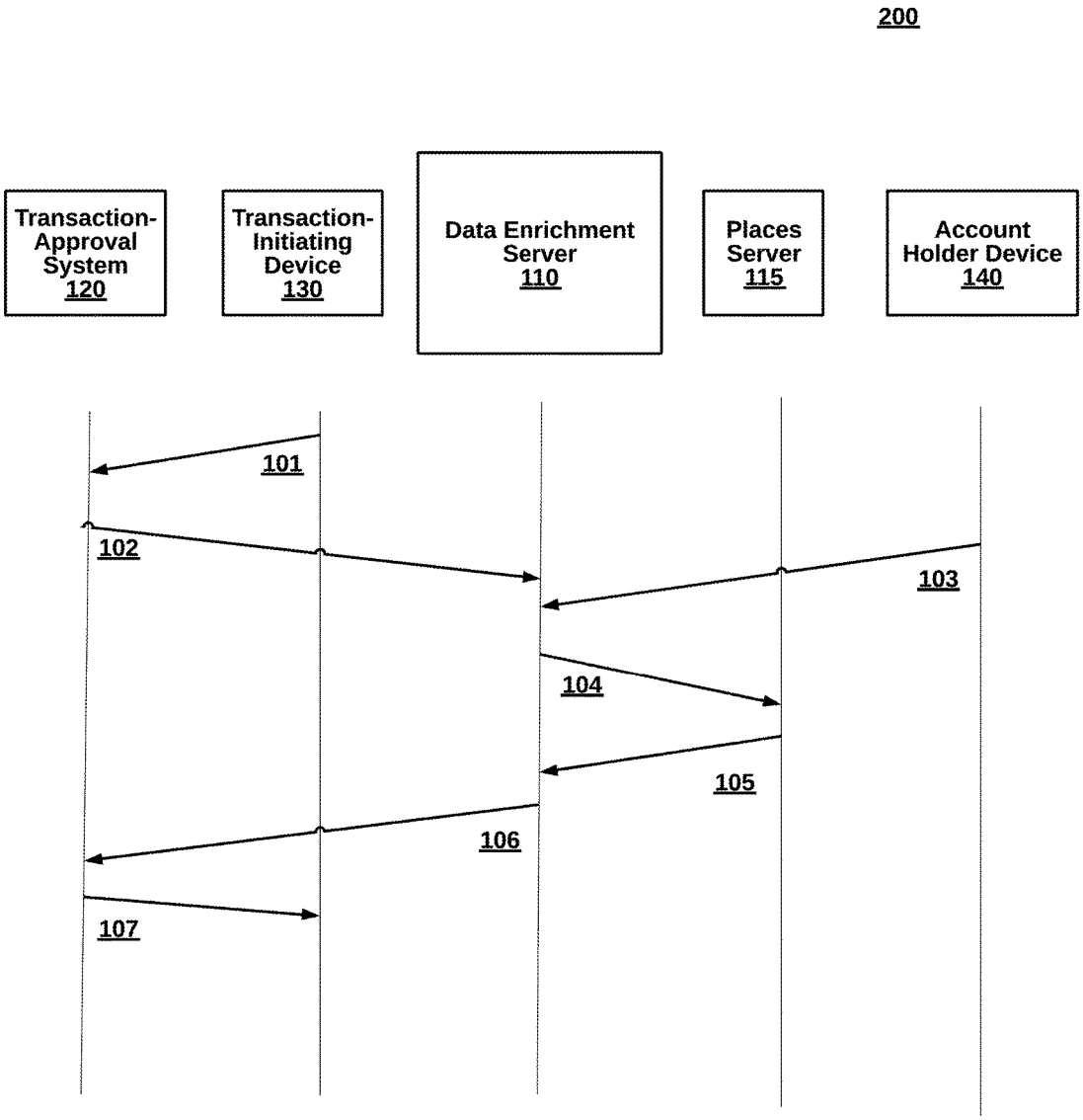

200
Transaction-Approval System 120
Transaction-Initiating Device 130
Data Enrichment Server 110
Places Server 115
Account Holder Device 140
101
102
103
104
105
106
107

FIG. 2

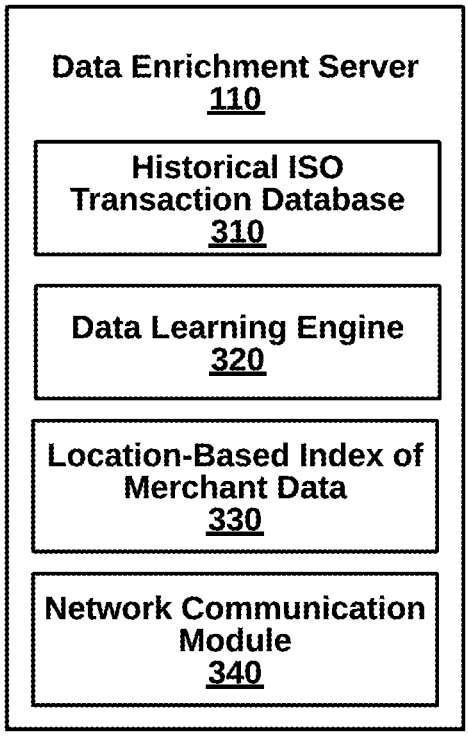

200
Data Enrichment Server
110
Historical ISO Transaction Database
310
Data Learning Engine
320
Location-Based Index of Merchant Data
330
Network Communication Module
340

FIG. 3

400

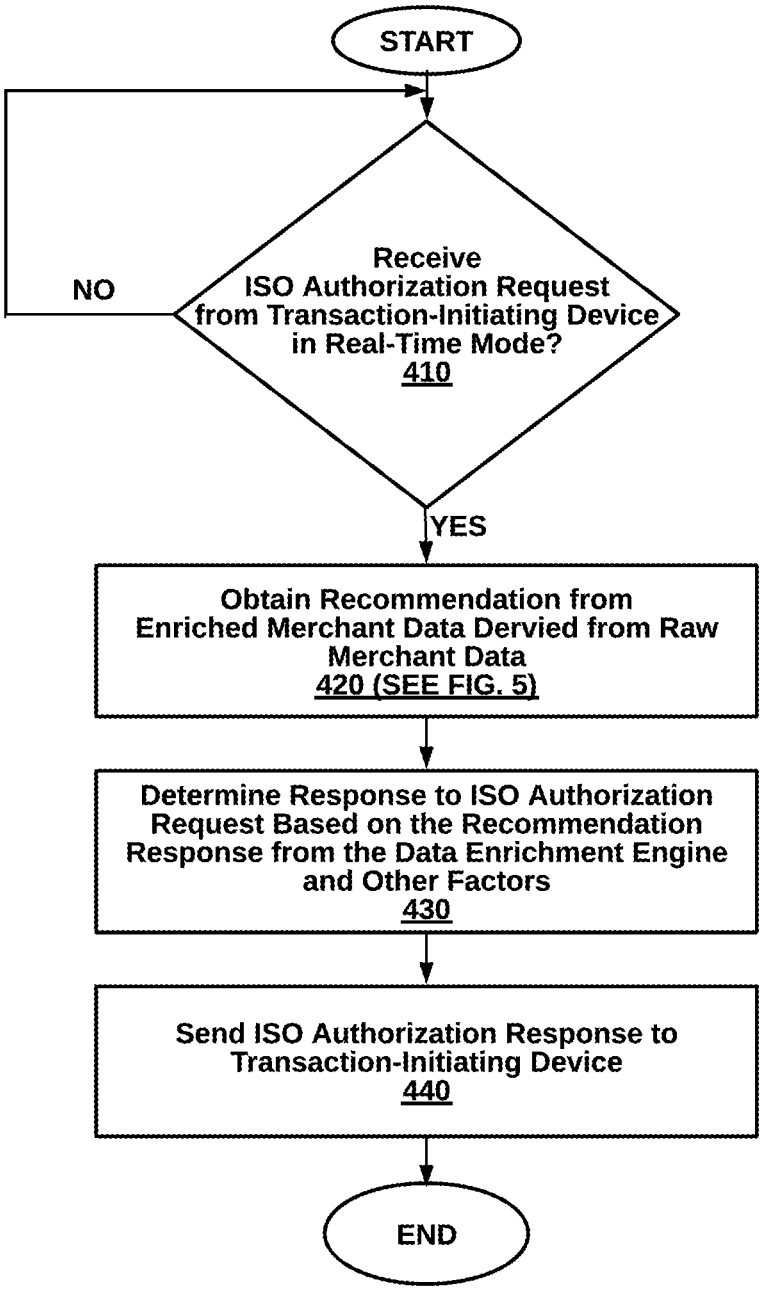

START
Receive ISO Authorization Request from Transaction-Initiating Device in Real-Time Mode? 410
NO
YES
Obtain Recommendation from Enriched Merchant Data Dervied from Raw Merchant Data 420 (SEE FIG. 5)
Determine Response to ISO Authorization Request Based on the Recommendation Response from the Data Enrichment Engine and Other Factors 430
Send ISO Authorization Response to Transaction-Initiating Device 440
END

FIG. 4

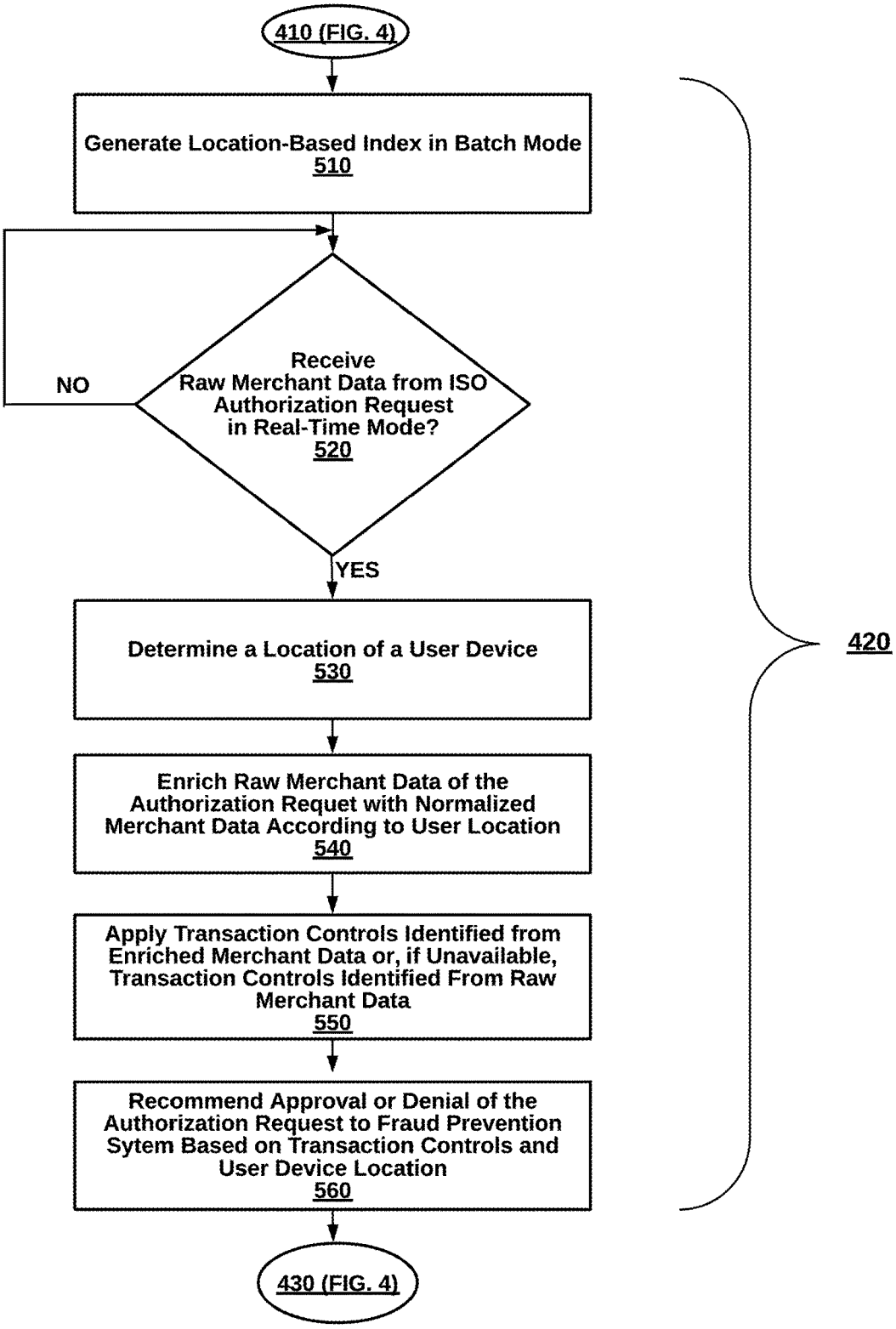

410 (FIG. 4)
Generate Location-Based Index in Batch Mode
510
Receive
Raw Merchant Data from ISO
Authorization Request
in Real-Time Mode?
520
NO
YES
Determine a Location of a User Device
530
Enrich Raw Merchant Data of the
Authorization Requet with Normalized
Merchant Data According to User Location
540
Apply Transaction Controls Identified from
Enriched Merchant Data or, if Unavailable,
Transaction Controls Identified From Raw
Merchant Data
550
Recommend Approval or Denial of the
Authorization Request to Fraud Prevention
Sytem Based on Transaction Controls and
User Device Location
560
430 (FIG. 4)
420

FIG. 5

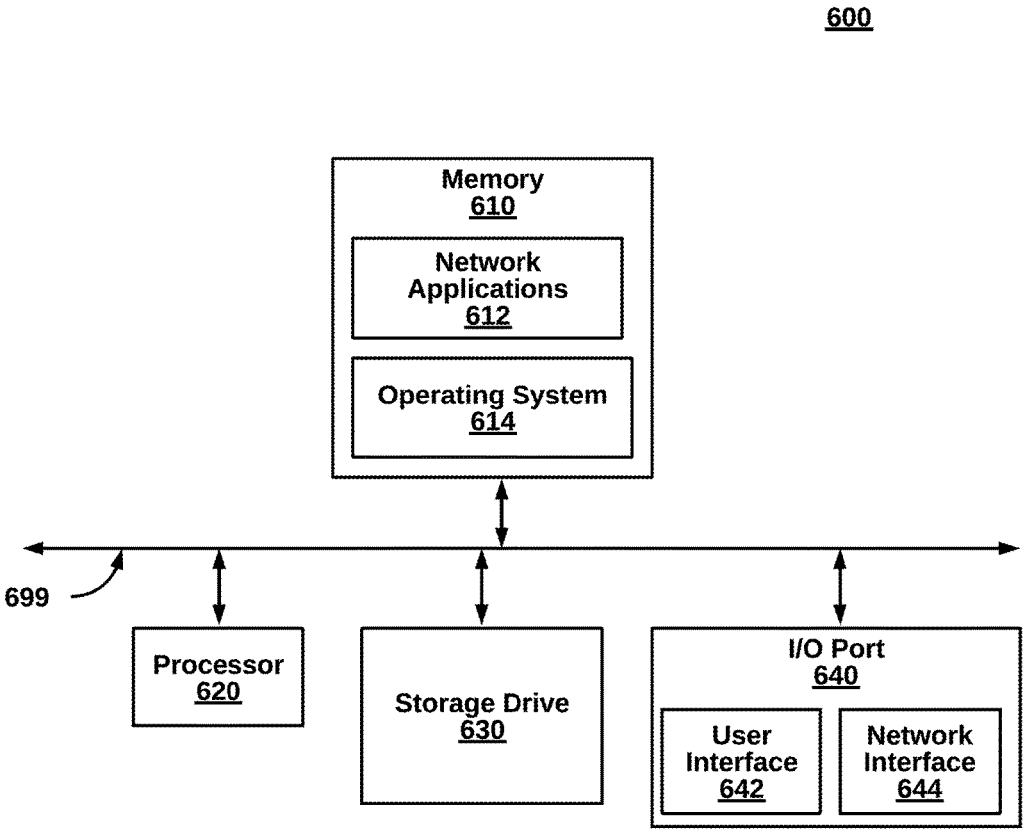

600
Memory
610
Network
Applications
612
Operating System
614
699
Processor
620
Storage Drive
630
I/O Port
640
User
Interface
642
Network
Interface
644

FIG. 6

REAL-TIME ENRICHMENT OF RAW MERCHANT DATA FROM ISO TRANSACTIONS ON DATA COMMUNICATION NETWORKS FOR PREVENTING FALSE DECLINES IN FRAUD PREVENTION SYSTEMS

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application claims priority under 35 USC 120 as a continuation-in-part of co-pending U.S. application Ser. No. 13/527,544 filed Jun. 19, 2012 entitled SYSTEM AND METHOD FOR PAYMENT AUTHORIZATION CONTROL, by Rachna Ahlawat, as a continuation-in-part to U.S. application Ser. No. 14/058,229 filed Oct. 19, 2013 entitled SYSTEM AND METHOD FOR AUTHORIZING A TRANSACTION BASED ON DYNAMIC LOCATION UPDATES FROM A USER DEVICE, by Vaduvur Bharghavan, which are hereby incorporated by reference in their entirety.

FIELD OF THE INVENTION

[0002] The invention relates generally, to computer networking security, and more specifically, to real-time enrichment of raw merchant data from an ISO (International Organization for Standardization) transaction for preventing a false decline in a fraud prevention system.

BACKGROUND

[0003] A major chilling effect on conducting online transactions is the vulnerability of transaction fraud from rogue network components. Rogue devices and rogue users can attempt to conduct fraudulent transactions without an account holder's permission. One solution to preventing transaction fraud is to maintain user accounts in a disabled state and selectively enabling accounts for any transactions to be considered, whether legitimate or not, as described in U.S. application Ser. No. 13/527,544.

[0004] However, once a user account is enabled, the content of a particular transaction still must be scrutinized for legitimacy. Unfortunately, many legitimate transactions are declined when fraud prevention methods are overly aggressive in the prevention of illegitimate transactions, and this can also have a chilling effect on online transactions.

[0005] What is needed is a robust technique for improving fraud prevention systems by reducing false declines in fraud prevention systems with real-time enrichment of raw merchant data from ISO transactions on a data communication network.

SUMMARY

[0006] To address the above-mentioned shortcomings, methods, computer-readable mediums, and devices are provided for real-time enrichment of raw merchant data from an ISO transaction for preventing a false decline in a fraud prevention system.

[0007] In one embodiment, a specific ISO authorization request having data fields formatted according to an ISO 8583 format, is received. The transaction can concern a specific mobile user and initiated by a specific merchant device at a merchant location. The merchant device controls values within the data fields formatted according to the specific ISO authorization request.

[0008] A geo-location of the specific mobile user associated is received from a specific mobile device authenticated by the specific mobile user. Raw merchant data is extracted from data fields of the specific ISO authorization request using the ISO 8583 format as a template for specific locations of the data fields. The raw merchant data of the specific ISO authorization request is replaced with enriched merchant data by searching a location-based index of normalized merchant data according to the mobile user location and the raw merchant data, wherein transaction controls available to a merchant name of the enriched merchant data is distinct from transaction controls available to a merchant name of the raw merchant data.

[0009] In an embodiment, responses are in real-time to the specific ISO authorization request with an approval recommendation based on the enriched merchant data responsive to a cache hit with respect to the location-based index. Also, responses are in real-time to the specific ISO authorization request with a denial recommendation based on the raw merchant data responsive to a cache miss to the location-based index.

[0010] Advantageously, the technical field of network security is improved by reducing falsely declined transactions.

BRIEF DESCRIPTION OF THE DRAWINGS

[0011] In the following drawings, like reference numbers are used to refer to like elements. Although the following figures depict various examples of the invention, the invention is not limited to the examples depicted in the figures.

[0012] FIG. **1** is a high-level block diagram illustrating a system for real-time enrichment of raw merchant data from an ISO transaction for preventing a false decline in a fraud prevention system, according to an embodiment.

[0013] FIG. **2** is a sequence diagram illustrating interactions between the components of the system of FIG. **1**, according to an embodiment.

[0014] FIG. **3** is a more detailed block diagram illustrating a data enrichment server of the system of FIG. **1**, according to some embodiments.

[0015] FIG. **4** is a high-level flow diagram illustrating a method for real-time enrichment of raw merchant data from an ISO transaction for preventing a false decline in a fraud prevention system, according to an embodiment.

[0016] FIG. **5** is a more detailed flow diagram describing the step of the fraud prevention system requesting a recommendation from the data enrichment server, according to an embodiment.

[0017] FIG. **6** is a block diagram illustrating an exemplary computing device, according to one embodiment.

DETAILED DESCRIPTION

[0018] Transaction validation servers, computer-implemented methods, and (non-transitory) computer-readable mediums for real-time enrichment of raw merchant data from an ISO transaction for preventing a false decline in a fraud prevention system, are disclosed.

[0019] The examples detailed herein are non-limiting and concise. For example, although fraud detection is referred to herein as a technology that is improved by the techniques disclosed below, many other technologies such as dispute resolution and card controls, are also improved. Moreover, merchant transactions in the ISO 8583 format for network

data packets can also be applied to non-merchant transactions and other packet formats. In addition to reducing false declines, fewer erroneous approvals are output.

[0020] I. System for Real-Time Enrichment of ISO Transactions (FIGS. **1-3**)

[0021] FIG. **1** is a high-level block diagram illustrating a system **100** for real-time enrichment of raw merchant data from an ISO transaction for preventing a false decline in a fraud prevention system, according to an embodiment. The system **100** primarily comprises a data enrichment server **110**, a transactional approval system **120**, a transaction-initiating device **130** and an account holder device **140**. Additional network components can also be part of the system **100**, such as firewalls, virus scanners, routers, switches, application servers, databases, as well as additional controllers, access points, access switches, stations, SDN (Software-Defined Networking) controllers, Wi-Fi controllers, and the like. The network components can be implemented as hardware, software, or a combination of both, for example, as described with respect to the computing environment of FIG. **6**.

[0022] Each of the primary components are coupled in communication through a network **199**. The account holder device **140** may be a mobile device that couples to an edge device **149** for access to the network **199**. In addition, the network **199** may be the Internet or a cellular network in one case and may be a hybrid network in another case.

[0023] The data enrichment server **110**, in one embodiment, receives a fraud recommendation request **101** with a copy of an ISO authorization request **101** and responds with a fraud recommendation response **101**. To determine a recommendation, the data enrichment server **110** can extract raw merchant data from the ISO authorization request. The raw merchant data is typically customized by a particular merchant and their business practice, or there is any protocol at all. Enriched merchant data, on the other hand, is normalized with known commercial names. It is the enriched merchant data from which more accurate fraud recommendations can be made, resulting in fewer false declines, among other advantages. In another embodiment, the data enrichment server **110** sends enriched merchant data to the transaction approval system **120** for fraud processing. While raw merchant data can have 2, 10 or more variations, enriched merchant data is coalesced under a single entry. When a customer wants to dispute a transaction at Walmart, for example, all the transactions and actions are accessible under a single commercial name rather than having to individually check each name and decipher raw merchant data.

[0024] The user location **103** for the account holder device **140** can be pushed or pulled and utilized to filter search results of a places server **119**. For example, a data field has WLMRT within close proximity to a known Walmart store, the custom abbreviation can be enriched to the common trade name. The location is preferably in real-time with data enrichment, but in some cases, is done asynchronously. GPS, Wi-Fi triangulation, IP address analyses, or other techniques at the account holder device **140** determines local geo-coordinates and sends to the data enrichment server **110**. In one case, the data enrichment server **110** uses algorithms to predict the location based on previous locations. In another case, the data enrichment server **110** infers location from the merchant location, IP address, or any other appropriate technique.

[0025] In some embodiments, the data enrichment server **110** is part of a third-party fraud detection system, separate from the fraud detection system of the transaction approval system **120**. This allows users to directly affect controls for fraud through the third-party access that is not available from the transaction approval system **120** fraud processes. The data enrichment server **110** is set forth in more detail with respect to FIG. **2** below.

[0026] The transactional approval system **120**, in an embodiment, is a backend to a payment authorization system for credit card transactions for a merchant at a POS. The financial transaction approval system can include an acquirer processor, a card network, an issuer processor, a card issuer, and an account host. Responsive to a transaction initiated at the merchant, the acquirer processor can send the ISO authorization request according to the ISO 8583 standard, including a x100 or a x200 message type, with a transaction card number, transaction card credentials, merchant information, transaction amount, and other mandatory and optional fields. The card network does validity checks on the ISO authorization request and involves any additional services the acquirer or issuer have signed up for (such as address validation, PIN validation, risk scoring, and the like), and then forward the ISO authorization request to the issuer processor. The issue processor can perform validity checks and invoke value-added services such as risk scoring and cardholder policy checks, before checking with an account host if a user account has adequate funds to satisfy a transaction request. The account host responds to the issuer processor with an approval or denial that the issuer processor can form into an ISO authorization response, along with a approve or denial reason code. The card network forwards the ISO authorization response to the acquirer processor, and in turn, back to the merchant at the POS. Many other approval systems are possible.

[0027] Conventional payment authorization systems typically block out the user device **140** from participation in approvals through payment controls. By contrast, the data enrichment server **110** is able to implement controls of the user device **140** by registering a user account with a third party administrating the data enrichment server **110**.

[0028] The transaction-initiating device **130**, can be a merchant device or other point of sale, where a merchant swipes a transaction card through a transaction card reader which uses transceiver coupled to the network **199** for transmitting an ISO authorization request to the transaction approval system **120** for approval.

[0029] The account holder device **140** can be a user device such as a mobile telephone, electronic payment device, an iPad, laptop computer, or the like. A user logs onto the data enrichment server **110** with authentication credentials to create a secure channel for location sharing, changing transaction controls, and managing transactions. In one implementation, a mobile application is downloaded to the account holder device **140** for communication with the data enrichment server **110**. In another embodiment, an operating system or Bluetooth-connected device communicates with the data enrichment sever **110**.

[0030] FIG. **2** is a sequence diagram illustrating interactions between the components of the system of FIG. **1**, according to an embodiment. Variations in the sequence are possible.

[0031] At interaction **101**, the transaction-initiating device **130** receives data from a payment card swipe by the mer-

chant or the user (or Apple Pay, an NFC contactless swipe, or otherwise) thereby initiating the network security techniques descried herein. Data packets including an ISO authorization request are sent to the transactional-approval system. The transmission channel can be, for example, an end-to-end wired connection, a Wi-Fi or other wireless connection, or a hybrid network.

[0032] At interaction **102**, a copy of the ISO authentication request is sent to the in order to receive a fraud recommendation and in response a use device location can be pulled (or pushed) from account holder device **140**. A search query is sent to the place server **115** at interaction **104** and a response is sent back at interaction **105**. Payment controls, fraud prevention scoring, or other processes can be applied at this point using enriched merchant data. At interaction **106**, a fraud recommendation is sent back to the transaction approval system **120**. At interaction, **107** the ISO authorization response is sent to the transaction-initiating device **130**. In response, a release of goods to the user can be allowed or disallowed by the merchant, in one example.

[0033] FIG. **3** is a more detailed block diagram illustrating a data enrichment server **110** of FIG. **1**, according to some embodiments. The data enrichment server **110** includes a historical ISO transactional database **310**, a data learning engine **320**, a location-based index of merchant data **330** and a network communication module **340**. The components can be implemented in hardware, software, or a combination.

[0034] The historical ISO transactional database **310** stores previous ISO authentication requests and responses for training the data learning engine **320**. The previous transactions can be limited to a specific user, a specific location (e.g., zip code, city or state), a specific transaction type (e.g., recurring transactions), or as otherwise needed for a specific implementation.

[0035] The location-based index of merchant data **330** is generated from the learning process as varying merchant names are coalesced under a single name, and payment controls are implemented through the single name. Being local to the data enrichment server **110**, one embodiment provides real-time look-up of enriched merchant data and when there is a cache miss, raw merchant data is used for making decisions. The enriched data can be retrieved form the places server **115**. Preferably, the data enrichment server **110** is under independent control from the transaction approval system **120**. As a result, the location-based index is controlled and leveraged by the user typically precluded from the ISO transaction data path.

[0036] The network communication module **340** can include a network interface, transceivers, antenna, protocol software, APIs and other aspects necessary

[0037] II. Methods for Real-Time Enrichment of ISO Transactions (FIGS. **4-5**)

[0038] FIG. **4** is a high-level flow diagram illustrating a method **300** for real-time enrichment of raw merchant data from an ISO transaction for preventing a false decline in a fraud prevention system, according to an embodiment. The method **300** can be implemented by, for example, the system **100** of FIG. **1**.

[0039] At step **410**, in response to an ISO authorization request is obtained from a transaction-initiating device in real-time mode from a merchant device initiating a transaction, a recommendation based on enriched merchant data derived from raw merchant data, is requested at step **420**.

[0040] At step **430**, a response to the ISO authorization request is determined based at least in part of the recommendation. In some implementation, other local controls and preferences are also taken into account, such as amount of credit available for a specific user.

[0041] At step **440**, the ISO authorization response is sent to the merchant. Results can be stored for batch processing at a later time. Additional verifications of the transaction or disputes submitted by users can also be stored for analyses.

[0042] FIG. **5** is a more detailed flow diagram describing the step **320** of the fraud prevention system requesting a recommendation from the data enrichment server from FIG. **3**, according to an embodiment.

[0043] At step **510**, a location-based index is generated in batch mode. At step **520**, responsive to receiving raw merchant data parsed from an ISO authorization request for a transaction in process, a location of a user device is determined at step **530**. At step **540**, raw merchant data is enriched with normalized merchant data according to the user location.

[0044] At step **550**, transaction controls (or transaction rules, or user preferences) can be identified and applied in order to make a recommendation, at step **560**. For example, a card present mode has different payment controls than a card not present mode. Co-location of a transaction card and a user device may be required in the card present mode. While the raw merchant data of WMRT345 may not be part of a location-based index, a look-up at a Google Places server or other database using the user device location can allow normalization of the merchant name to Walmart, a name that is part of the location-based index. Additional data can also be gleaned from the Google Places server such as merchant location, and factors for determining terminal type. The additional data may further affect the payment controls applied to make an even more accurate recommendation. As a result, false declines of the transaction are prevented. Many other examples are possible.

[0045] III. Generic Computing Device (FIG. **6**)

[0046] FIG. **6** is a block diagram illustrating an exemplary computing device **600** for use in the system **100** of FIG. **1**, according to one embodiment. The computing device **500** is an exemplary device that is implementable for each of the components of the transaction validation server unit **110**, including the historical transaction database **310**, account configuration module **320**, the deviation determination engine **330**, and network communication module **340**. Additionally, the computing device **500** is merely an example implementation itself, since the system **100** can also be fully or partially implemented with laptop computers, tablet computers, smart cell phones, Internet appliances, and the like.

[0047] The computing device **600**, of the present embodiment, includes a memory **610**, a processor **620**, a storage drive **630**, and an I/O port **640**. Each of the components is coupled for electronic communication via a bus **699**. Communication can be digital and/or analog, and use any suitable protocol.

[0048] The memory **610** further comprises network applications **512** and an operating system **614**. The network applications **612** can include a web browser, a mobile application, an application that uses networking, a remote application executing locally, a network protocol application, a network management application, a network routing application, or the like.

[0049] The operating system **614** can be one of the Microsoft Windows®. family of operating systems (e.g., Windows 95, 98, Me, Windows NT, Windows 2000, Windows XP, Windows XP x64 Edition, Windows Vista, Windows CE, Windows Mobile), Windows 7, Windows 8, Linux, HP-UX, UNIX, Sun OS, Solaris, Mac OS X, Alpha OS, AIX, IRIX32, or IRIX64. Other operating systems may be used. Microsoft Windows is a trademark of Microsoft Corporation.

[0050] The processor **620** can be a network processor (e.g., optimized for IEEE 802.11), a general-purpose processor, an application-specific integrated circuit (ASIC), a field programmable gate array (FPGA), a reduced instruction set controller (RISC) processor, an integrated circuit, or the like. Qualcomm Atheros, Broadcom Corporation, and Marvell Semiconductors manufacture processors that are optimized for IEEE 802.11 devices. The processor **620** can be single core, multiple core, or include more than one processing elements. The processor **620** can be disposed on silicon or any other suitable material. The processor **620** can receive and execute instructions and data stored in the memory **610** or the storage device **630**.

[0051] The storage device **630** can be any non-volatile type of storage such as a magnetic disc, EEPROM, Flash, or the like. The storage device **630** stores code and data for applications.

[0052] The I/O port **640** further comprises a user interface **642** and a network interface **644**. The account holder interface **642** can output to a display device and receive input from, for example, a keyboard. The network interface **644** connects to a medium such as Ethernet or Wi-Fi for data input and output. In one embodiment, the network interface **644** includes IEEE 802.11 antennae.

[0053] Many of the functionalities described herein can be implemented with computer software, computer hardware, or a combination.

[0054] Computer software products (e.g., non-transitory computer products storing source code) may be written in any of various suitable programming languages, such as C, C++, C#, Java, JavaScript, PHP, Python, Perl, Ruby, and AJAX. The computer software product may be an independent application with data input and data display modules. Alternatively, the computer software products may be classes that are instantiated as distributed objects. The computer software products may also be component software such as Java Beans (from Sun Microsystems) or Enterprise Java Beans (EJB from Sun Microsystems).

[0055] Furthermore, the computer that is running the previously mentioned computer software may be connected to a network and may interface to other computers using this network. The network may be on an intranet or the Internet, among others. The network may be a wired network (e.g., using copper), telephone network, packet network, an optical network (e.g., using optical fiber), or a wireless network, or any combination of these. For example, data and other information may be passed between the computer and components (or steps) of a system of the invention using a wireless network using a protocol such as Wi-Fi (IEEE standards 802.11, 802.11a, 802.11b, 802.11e, 802.11g, 802.11i, 802.11n, and 802.ac, just to name a few examples). For example, signals from a computer may be transferred, at least in part, wirelessly to components or other computers.

[0056] In an embodiment, with a Web browser executing on a computer workstation system, a user accesses a system on the World Wide Web (WWW) through a network such as the Internet. The Web browser is used to download web pages or other content in various formats including HTML, XML, text, PDF, and postscript, and may be used to upload information to other parts of the system. The Web browser may use uniform resource identifiers (URLs) to identify resources on the Web and hypertext transfer protocol (HTTP) in transferring files on the Web.

[0057] This description of the invention has been presented for the purposes of illustration and description. It is not intended to be exhaustive or to limit the invention to the precise form described, and many modifications and variations are possible in light of the teaching above. The embodiments were chosen and described in order to best explain the principles of the invention and its practical applications. This description will enable others skilled in the art to best utilize and practice the invention in various embodiments and with various modifications as are suited to a particular use.

We claim:

1. A computer-implemented method in a data enrichment server device improving a fraud prevention system on a data communication network by reducing false declines associated with real-time approval of ISO transactions based on enrichment of raw merchant data, the method comprising:

receiving in real-time, at a network communication interface of the data enrichment server device, a specific ISO authorization request having data fields formatted according to an ISO 8583 format, the transaction concerning a specific mobile user and initiated by a specific merchant device at a merchant location, wherein the merchant device controls values within the data fields formatted according to the specific ISO authorization request;

receiving, at the network communication interface, a geo-location of the specific mobile user associated with the specific ISO authorization request from a specific mobile device authenticated by the specific mobile user;

parsing, with a processor of the data enrichment server, raw merchant data from data fields of the specific ISO authorization request using the ISO 8583 format as a template for specific locations of the data fields;

augmenting the raw merchant data of the specific ISO authorization request with enriched merchant data by searching a location-based index of normalized merchant data according to the mobile user location and the raw merchant data, wherein transaction controls available to a merchant name of the enriched merchant data are distinct from transaction controls available to a merchant name of the raw merchant data; and

responding in real-time to the specific ISO authorization request with an approval recommendation based on the enriched merchant data responsive to a cache hit with respect to the location-based index and responding in real-time to the specific ISO authorization request with a denial recommendation based on the raw merchant data responsive to a cache miss to the location-based index.

2. The method of claim **1**, further comprising:

determining the merchant device location from the ISO authorization request by parsing the raw merchant data from the ISO authorization request;

determining a mismatch between the merchant device location and the user device location; and

recommending denial to the specific ISO authorization request.

3. The method of claim **1**, further comprising:

in response to the cache miss with respect to the location-based index, retrieving enriched merchant data from an external data source; and

updating the location-based index by storing the enriched merchant data.

4. The method of claim **1**, wherein the step of receiving the geographic location of the user device comprises:

responsive to receiving the specific ISO authorization request, sending a request to the user device for the user device location.

5. The method of claim **1**, wherein the step of receiving the geographic location of the user device comprises:

prior to receiving the specific ISO authorization request, receiving the user device location.

6. The method of claim **1**, further comprising:

generating in batch mode, at a processor of the network communication interface, a location-based index of merchant data from a batch of previous ISO transactions on the data communication network.

7. The method of claim **1**, wherein the augmenting step comprises:

augmenting the raw merchant data of the specific ISO authorization request with enriched merchant data by searching a location-based index of normalized merchant data according to the mobile user location and the raw merchant data, wherein transaction controls available to a merchant name of the enriched merchant data are distinct from transaction controls available to a merchant name of the raw merchant data, and wherein the normalized merchant data includes a normalized merchant name, and a normalized merchant address.

8. A non-transitory computer-readable medium comprising source code that, when executed by a processor, performs a computer-implemented method in a data enrichment server device of a fraud prevention system on a data communication network for reducing false declines with real-time approval of ISO transactions based on enrichment of raw merchant data, the method comprising:

receiving in real-time, at a network communication interface of the data enrichment server device, a specific ISO authorization request having data fields formatted according to an ISO 8583 format, the transaction concerning a specific mobile user and initiated by a specific merchant device at a merchant location, wherein the merchant device controls values within the data fields formatted according to the specific ISO authorization request;

receiving, at the network communication interface, a geo-location of the specific mobile user associated with the specific ISO authorization request from a specific mobile device authenticated by the specific mobile user;

parsing, with a processor of the data enrichment server, raw merchant data from data fields of the specific ISO authorization request using the ISO 8583 format as a template for specific locations of the data fields;

augmenting the raw merchant data of the specific ISO authorization request with enriched merchant data by searching a location-based index of normalized merchant data according to the mobile user location and the raw merchant data, wherein transaction controls available to a merchant name of the enriched merchant data is distinct from transaction controls available to a merchant name of the raw merchant data; and

responding in real-time to the specific ISO authorization request with an approval recommendation based on the enriched merchant data responsive to a cache hit with respect to the location-based index and responding in real-time to the specific ISO authorization request with a denial recommendation based on the raw merchant data responsive to a cache miss to the location-based index.

* * * * *