May 2023

VISA WARRANTY SHIELD

PAVAN NAGARAJA RAO
VISA

RUCHIRA CHAKRABARTY
VISA

ZAKIRHUSSAIN KADER MOHIDEEN
VISA

ANISH RADHAKRISHNAN
VISA

VISA WARRANTY SHIELD

VISA

INVENTORS:

- **PAVAN NAGARAJA RAO**
- **RUCHIRA CHAKRABARTY**
- **ZAKIRHUSSAIN KADER MOHIDEEN**
- **ANISH RADHAKRISHNAN**

TECHNICAL FIELD

[0001] The present subject matter is, in general, related to processing consumer claims against purchased products, and particularly, to techniques for providing efficient and effective warranty claim management.

BACKGROUND

[0002] A manufacturing organization produces products and then supplies them to dealers or sellers. The dealers or sellers distribute the products to consumers/customers, or the consumers purchase the products from the dealers or sellers. Upon purchasing a product, a consumer receives an invoice for the purchased product, which may include associated warranty information of the product (if applicable). The invoice can be provided as a physical copy or a digital/soft copy. Generally, the warranty is a contractual obligation by a manufacturer, an Original Equipment Manufacturer (OEM), or a seller of the product to be liable to customers in the event of premature product failure inability of the product to function as expected, and like.

[0003] After the purchase, in order to get warranty on the purchased product, the consumer/customer has to put an extra effort. For example, after the purchase, the consumer is usually asked to fill in an online/offline warranty form with purchase details. Sometime, the consumer may be asked to send a copy of the filled form and/or details of purchase to the manufacturer. Sometimes these invoices and/or warranty forms may get misplaced e.g., due to the ignorance from the consumer, and/or sometimes the warranty may expire before the consumer realizes it, which makes it difficult to claim the benefits that were guaranteed to the consumer at the time of purchasing the product. Sometimes, when the consumer submits warranty form to the merchant or seller, the merchant/seller may take a long time to address such warranty issues. This causes dissatisfaction of the consumer towards the manufacturer.

[0004] In the existing practice, the process of registering product warranties is often manual and paper-based, leading to a cumbersome experience for consumers. Nowadays, many organizations have adopted digital channels for marketing and selling their products. However, there is little effort, or no effort made by the organizations to digitize the warranty tracking process. In conventional practice, there is no single application or interface that can act as a bridge between the consumer or OEM or sellers/dealers for providing services such as feedback, promotions, cross sell/upsell, installation, usage guidance, common trouble shooting tips and guidance to locate the nearest authorized service center. The warranty claiming process

can also cause friction between the consumer and the manufacturer/seller. For instance, when the consumer purchases any product from a seller /dealer, the seller/dealer provides an invoice and an associated warranty card/paper to the consumer. However, the seller/dealer may forget to put a physical stamp over the warranty card. As a result, the consumer may not claim the warranty, resulting in friction between the consumer and the manufacturer/seller.

[0005] Additionally, some organizations do not monitor or track warranties for sold products, leading to consumer dissatisfaction when trying to claim the warranty. This is often due to the drain on revenue that warranty claims can cause to organizations. However, neglecting warranty claims can have a significant impact on consumer loyalty and repeat purchases. Unsatisfied consumers are less likely to recommend products to their friends and family, leading to a decline in sales and consumer retention.

[0006] To address the above discussed issues, a single platform should be implemented that allows consumers, manufacturers, and dealers, sellers, retailers to track the warranty status of purchased products and reduce the friction in warranty registration and warranty claiming process.

[0007] The information disclosed in the background section of the disclosure 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.

BRIEF DESCRIPTION OF THE DRAWINGS

[0008] The accompanying drawings, which are incorporated in and constitute a part of this disclosure, illustrate exemplary embodiments and, together with the description, explain the disclosed principles. In the figures, the left-most digit(s) of a reference number identifies the figure in which the reference number first appears. The same numbers are used throughout the figures to reference features and components. Some embodiments of device or system and/or methods in accordance with embodiments of the present subject matter are now described, by way of example only, and with reference to the accompanying figures, in which:

[0009] **Figs. 1A and 1B** show schematic representations **100a**, **100b** of an exemplary environment comprising a warranty management system **101** to reduce friction in a warranty

registration process and warranty claiming process, in accordance with some embodiments consistent with the present disclosure.

[0010] **Fig. 2** shows a schematic representation **200** showing a sequence of steps involved in warranty registration and claiming process, in accordance with some embodiments consistent with the present disclosure.

[0011] **Fig. 3** illustrates a sequence diagram for updating a warranty shield database, in accordance with some embodiments consistent with the present disclosure.

[0012] **Fig. 4** illustrates a sequence diagram of communication between the warranty management system **101** and an e-commerce portal **111**, in accordance with some embodiments consistent with the present disclosure.

[0013] **Fig. 5** illustrates a sequence diagram of communication between the warranty management system **101** and OEMs **115**, in accordance with some embodiments consistent with the present disclosure.

[0014] **Fig. 6** illustrates a sequence diagram of communication between the warranty management system **101** and the user device **107** associated with a user, in accordance with some embodiments consistent with the present disclosure.

[0015] **Fig. 7** shows a flow chart of a method for reducing a friction in a warranty registration process and warranty claiming process, in accordance with some embodiments consistent with the present disclosure.

[0016] **Fig. 8** illustrates a block diagram of an exemplary computer system **800** for implementing embodiments consistent with the present disclosure.

[0017] The figures depict embodiments of the disclosure for purposes of illustration only. One skilled in the art will readily recognize from the following description that alternative embodiments of the structures and methods illustrated herein may be employed without departing from the principles of the disclosure described herein.

DESCRIPTION OF THE DISCLOSURE

[0018] 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.

[0019] 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 spirit and the scope of the disclosure.

[0020] 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 device or system or apparatus proceeded by “comprises… a” does not, without more constraints, preclude the existence of other elements or additional elements in the device or system or apparatus.

[0021] 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.

[0022] The terms "including", "comprising", “having” and variations thereof mean "including but not limited to", unless expressly specified otherwise. The terms “user” and “customer” have been used interchangeably throughout the disclosure. In the present disclosure, the term “offers” “promotions” and “promotional offers” have been used interchangeably throughout the disclosure. The offers/promotions may include discounts, incentives, rewards, rebates, gifts, cashbacks, coupons, reward points, or any such benefit which can be availed/redeemed upon satisfaction of certain conditions.

[0023] The present disclosure discloses a warranty management system for reducing the friction in warranty registration and warranty claim process to improve the overall consumer experience. The proposed system simplifies the warranty registration and warranty claiming processes, leading to higher consumer satisfaction and loyalty, better management of warranty

claims for organizations so as to enable them to provide faster and more efficient services to the consumers eventually leading to increased sales, consumer retention, and a positive reputation for the organization.

[0024] The proposed warranty management system may communicate with merchant/retailer, user/customer/consumer, and/or Original Equipment Manufacturer (OEM). Specifically, the consumer may purchase a product and initiate a transaction for the payment. The transaction may be authorized by a network and Merchant Category code is picked up by the network. The warranty management system may send a notification to the consumer for requesting confirmation on the purchase. In response, the consumer may confirm the purchase of the product. Subsequently, the warranty management system may call e-commerce portal and request purchase details such as invoice, customer support information, warranty information etc. All the purchase details are retrieved by a user device associated with the consumer. Finally, the warranty management system may call OEM and provide all the details for the future access.

[0025] **Fig. 1** shows a schematic representation **100a** of an exemplary environment comprising a warranty management system **101** to reduce friction in a warranty registration process and warranty claiming process, in accordance with some embodiments consistent with the present disclosure.

[0026] As shown in **Fig. 1A**, the exemplary environment may comprise a Warranty Management System (WMS) **101**, a user **103**, one or more payment cards **105** and a user device **107** associated with the user **103**, an e-commerce portal **111**, a network **113**, and an Original Equipment Management (OEM) **115**. The warranty management system **101** may be a central platform or a web service that communicates with the e-commerce portal **111**, the user **103**, and the OEM **115**. The warranty management system **101** may help in warranty registration process and warranty claiming process for users **103** when the users **103** purchase any products from the sellers/dealers or manufacturers. The user **103** may be a customer or consumer and/or cardholder who purchases products/gets service from the merchants, sellers/dealers, and/or manufacturers. Further, user **103** may possess one or more payment cards **105** issued by same or different issuers. As an example, the issuers may include, without limitation, a bank, a financial institution, and the like. As an example, one or more payment cards **105** may include, without limitation, a debit card, a credit card, a prepaid card, a virtual card, and the like. The user **103** may possess the user device **107**. As an example, the user device **107** may include,

without limitation, a smart phone, a laptop, a desktop, a computer, and the like. The user device **107** may include at least one memory communicatively coupled with at least one processor (not shown in **Fig. 1A**) to perform various functionalities. An application **109** may be installed in the user device **107**. As an example, the application **109** may be a mobile software application that allows the user device **107** to perform specific tasks. For instance, in the present disclosure, the application **109** may be named as "a warranty shield application" which is installed in the user device **107** to keep track of the purchases made by the user **103**. The user device **107** may communicate with the warranty shield system **101** via the network **113**. The network **113** may include one or more private and/or public networks such as the Internet, a local area network (LAN), a wide area network (WAN), Metropolitan Area Network (MAN), a cellular voice/data network, and/or other such types of wireless/wired communication network.

[0027] The e-commerce portal **111** may be an online platform which allows different business entities like customers, manufacturers, sellers, dealers, suppliers, and like to interact and perform instant transactions in a more intuitive manner. In other words, the e-commerce portal **111** may help in online buying or selling of products using the internet. As an example, the e-commerce portal **111** may include, without limitation, online stores such as Amazon™, Flipkart™, Shopify™, Myntra™, eBay™, Quikr™ etc. The Original Equipment Manufacturers (OEMs) **115** may be manufacturers that manufacture various products which the sellers/dealers may sell via the e-commerce portal **111**.

[0028] In an embodiment, the user **103** may purchase a product from the e-commerce portal **111** and make payment using one of the payment cards **105**. The user **103** may purchase a product through the e-commerce portal **111** with a "Card Not Present (CNP) transaction". As an example, the CNP transaction is a payment card transaction performed by the user **103**, where a cardholder is typically not physically present at the time of the purchase. The transaction request may be routed to the warranty management system **101** through the network **113**. The network **113** may receive or fetch a Merchant category Code (MCC) contained in the authorization request and may authorize the transaction. The MCC may be a four-digit number issued by a card issuer. The MCC may be used to classify merchants by the type of goods or services they provide. For example, if the MCC code is 5732, then the merchant may be a seller of electronic devices.

[0029] When the transaction is authorized by the network **113**, the warranty management system **101** may send a push notification (e.g., in the form a text or audio alert) to the user device **107** and request the user **103** to confirm the purchase made. Subsequently, the user **103** may send confirmation of the purchase made using the warranty shield application **109** to the warranty management system **101**.

[0030] After receiving the confirmation from the user device **107**, the warranty management system **10**1 makes a Hyper Text Transfer Protocol (HTTP) call to the e-commerce portal **111** and requests purchase details of the product. The e-commerce portal **111** may redirect the request to a webserver (not shown). The webserver may provide the purchase details to the e-commerce portal **111**. Subsequently, the e-commerce portal **111** may send purchase details of the product to the warranty management system **101**. As an example, the purchase details from the web server of the e-commerce portal **111** may include, without limitation, a soft copy of invoice of the product purchased, customer support information, warranty information of the purchased product, and the like. The customer support information may include, without limitation, support center details, nearest location of support center, a customer care toll free number, a soft copy of the manual to indicate how to use the purchased product, troubleshooting tips, and the like.

[0031] The e-commerce portal **111** may send the purchase details (i.e., the soft copy of the invoice, the customer support information, and the warranty information) to the warranty management system **101**. Subsequently, the warranty shield application **109** installed in the user device **107** may retrieve the purchase details from the warranty management system **101** (e.g., using a backend process). The warranty management system **101** may make a HTTP call to the OEM **115** and provide the purchase details. As a result, the user **103** may possess the purchase details of the product and the OEM **115** may also possess purchase details of the product purchased by the user **103**. Consequently, the OEM **115** may keep track of the warranty for the purchased product and similarly, the user **103** may need not fill the physical form and submit to the OEM **115** for warranty registration and/or warranty claiming.

[0032] In an alternative embodiment, shown in a schematic representation **100b** of **Fig. 1B**, the user **10**3 may purchase a product at the retailer's/merchant's place. As an example, the user **103** may physically visit any store or shop, purchase a product using a payment card **105**, and make payment for the purchased product by swiping the payment card **105** on a Point of Sale (POS) terminal installed at the retailer's/merchant's place. The transaction request may be

routed to the warranty management system **101** through the network **113**. The network **113** may receive or fetch a MCC code contained in the authorization request and may authorize the transaction. As mentioned above, the MCC may be used to classify merchants by the type of goods or service they provide.

[0033] When the transaction is authorized by the network **113**, the warranty management system **101** may send a push notification (e.g., in the form of a text or audio alert) to the user device **107** and request the user **103** to confirm the purchase made. Subsequently, the user **103** may send confirmation on the purchase made using the warranty shield application **109** to the warranty management system **101**. After receiving the confirmation from the user device **103**, the warranty management system **101** may prompt the user **103** to capture or take a picture of the invoice, an image of the product, a serial number or a product ID of the product using the warranty shield application **109** installed in the user device **107**. The user **103** may capture the aforementioned information using the warranty shield application **109** and subsequently, send all the captured information (i.e., image of invoice, image of the purchased product, serial number of product ID of the purchased product) to the warranty management system **101** (e.g., using a backend process). The warranty management system **101** may make a HTTP call to the OEM **115** and provide the purchase details. As a result, the user **103** may possess the purchase details of the product and the OEM **115** may also prosses purchase details of the product purchased by the user **103**. Consequently, the OEM **115** may keep track of the warranty for the purchased product and similarly, the user **103** may need not fill the physical form and submit to the OEM **115** for warranty registration and/or warranty claiming.

[0034] **Fig. 2** shows a schematic representation **200** showing a sequence of steps involved in warranty registration and claiming process, in accordance with some embodiments consistent with the present disclosure.

[0035] At **step 1** (S1), a merchant may call one or more Application Programming Interfaces (APIs) which may be exposed by a payment gateway. For instance, the payment gateway may offer a complete portfolio of online and in-person services for simplifying and automating the payments. In an aspect, the payment gateway may be “CyberSource” which is a global payment gateway that enables online card payments (for example debit or credit card payments) around the world. The CyberSource processes each transaction securely from start to finish.

[0036] At **step 2** (S2), a Common Gate Keeper (CGK) may receive a transaction request from the merchant and apply security controls (for example, API gateway). Subsequently, the CGK may forward the call/request to an Orchestrator (L1) and a Policy Decision System (PDS). The PDS may be used in merchant validation and configuration, authentication, authorization, and rate limiting. The L1 Orchestrator may integrate and manage end-to-end payment processes including authorizing payments, and/or routing of transactions etc. The transaction request forwarded from the CGK to the PDS may be in encrypted form (for example Simple Commerce Message Protocol (SCMP) request). At **step 3** (S3), the CGK may call PDS. The PDS decrypts the received request, validate user credentials for authorization, and perform configuration database lookup to get new merchant configuration attributes such as horizon_enabled, datacenter_affinity, etc. Further, the PDS may convert the received SCMP request to Java Script Object Notation (JSON) and may include the JSON structured data in the response sent to the CGK.

[0037] At **step 4** (S4), the L1 orchestrator may decrypt the received call and perform token management as indicated in the **step 6** (S6). The token management is an imperative step for the users **103** to add an extra layer of security to their transaction information or data. Further, a payment lookup may also be performed. The payment lookup may help in searching of specific transaction, it may indicate the transaction ID and date of the purchase. This payment lookup may be used to retrieve more information about one transaction after searching for a range of transactions.

[0038] At **step 5** (S5), the L1 Orchestrator may then forward the data to a L2 Orchestrator. The L2 Orchestrator, based on the type of payment (for example, credit or debit or risk etc.), may add MCC, perform Bank Identification Number (BIN) lookup, and may select suitable gateway. The BIN look up feature may help in accessing the BIN of the payment card. In other words, the BIN lookup may determine whether the payment card used for transaction is the debit card or the credit card. At **step 6** (S6), based on the token management service, decryption of the request, BIN lookup and payment Orchestration services, the transaction is performed normally.

[0039] At **step 7** (S7), a Platform Connect (PC) may validate the transformation (i.e., conversion to acquirer/processor format) and transaction persistence. The transaction may be passed to a PC daemon. The PC daemon may run continuously as a background process in the transaction, and it may handle periodic requests. The PC daemon may respond to the received

transaction request, or it may forward the transaction request to an Integrated Payment Systems (IPS). At **step 8** (S8), the warranty management system **101** may ask the user **103** to subscribe to one or more categories produced by the L2 Orchestrator. For example, the one or more categories may include Kafka topics. The subscription data may be ingested into an underlying database of the warranty management system **101**. The Kafka topics are the categories used to organize messages. The messages may be sent to and read from the specific topics. In Kafka topics, producers write data to topics and the consumers read data from the topics.

[0040] At **step 9** (S9), the warranty management system (WMS) **101** may be connected to a forward proxy server in order to connect with the e-commerce portal **111**, the OEM **115**, and the user device **107**. At **step 10** (S10), the warranty management system **101** may trigger a push notification to the user device **107** based on the application logic (shown in Fig. 7). The factors that trigger the notification to the user device **107** may be based on the MCC and other details captured from the Kafka topics.

[0041] At **step 11**, **step 12,** and **step 13** (S11, S12 and S13), secure communication may be performed between the forward proxy and the user device **107**, the OEMs **115**, and the e-commerce portal **111** respectively. The communication may be secured using API authentication. At **step 14** (S14), a User Interface (UI) (referred to as "WMS UI") may be provided for the OEMs **115**, merchant, and e-commerce portal **111** are managed for reporting purposes. Further, an acquirer may communicate with the IPS, and subsequently, the IPS may communicate with the issuer and may map every transaction to a particular payment ID.

[0042] **Fig. 3** illustrates a sequence diagram for updating a warranty shield database, in accordance with some embodiments consistent with the present disclosure.

[0043] At **step 1**, the warranty management system **101** may check or fetch enriched transaction or payment related information by sending a message to a server (for e.g., a Kafka server) associated with the L2 Orchestrator of the CyberSource. For instance, the enriched transaction information may comprise additional information added to the raw transaction data that already exists. For example, the additional information may include, without limitation, merchant details (for example, name, location, and category), payment details (for example payment method used), and the like.

[0044] At **step 2**, the warranty management system **101** may update the database by writing the transaction details (fetched from the server) into the database.

[0045] **Fig. 4** illustrates a sequence diagram of communication between the warranty management system **101** and the e-commerce portal **111**, in accordance with some embodiments consistent with the present disclosure.

[0046] Initially, the warranty management system **101** may connect with a forward proxy. As an example, the forward proxy may be a server. The forward proxy may be an intermediary node which is located in between the e-commerce portal **111** and the warranty management system **101**. In the transaction, instead of validating a client request and sending it to directly to a web server, the forward proxy server may evaluate the request, take required actions, and route the request to the destination.

[0047] **At step 1**, the warranty management system **101** connects with the forward proxy and makes HTTP call for requesting the purchase details as indicated in **step 2**. The forward proxy may evaluate the HTTP call request and route the HTTP call request to the e-commerce portal **111**. In response to the HTTP call by the warranty management system **101**, the e-commerce portal **111** may communicate with the web server. The web server may provide required information to the e-commerce portal **111**. The e-commerce portal **111** may send a response to the forward proxy server. The forward proxy may forward the response to the warranty management system **101** as indicated in the **step 3**. As an example, the response may include, without limitation, details of the invoice, the customer support information, and the warranty information, and other information related to purchased product.

[0048] **Fig. 5** illustrates a sequence diagram of communication between the warrant management system **101** and the OEMs **115**, in accordance with some embodiments consistent with the present disclosure.

[0049] **At step 1**, the warranty management system **101** may connect with the forward proxy and make a HTTP call for purchase details. The forward proxy may evaluate the HTTP call request and route the HTTP call request to the OEMs **115** as indicated in **step 2**. In response to the HTTP call from the warranty management system **101**, the OEMs **115** may send a response (either directly or via the forward proxy) to the warranty management system **101** as indicated in the **step 3**. As an example, the response may include HTTP 200 OK success status response

which indicates that the request has been successfully accepted and permission for communication is granted. Subsequently, the warranty management system **101** may provide details of the purchase such as serial number, the customer support information, and warranty information to the OEMs **115**.

[0050] **Fig. 6** illustrates a sequence diagram of communication between the warranty management system **101** and the user device **107** associated with a user, in accordance with some embodiments consistent with the present disclosure.

[0051] **At step 1**, the user device **107** may subscribe to a push notification service (e.g., a service which sends push notifications in the form of text or audio alert). The warranty management system **101** may connect with the forward proxy (**step 2**) and the forward proxy may make a HTTP call to the push notification service, as indicated in **step 3**. It may be noted that initially, as shown in **step 3**. At **step 4**, the push notification service may send push notification to the user device **107** requesting the user to confirm the purchase made. At **step 5**, the user device **107** may send an update message to the warranty management system **101** (e.g., using warranty shield application **109** installed in the user device **107)**, the update message may be indicative of purchase confirmation and may comprise the purchase details of the product.

[0052] Subsequently, at **step 6**, the warranty management system **101** may provide response to the user device **107**. For example, the response may include product warranty information.

[0053] **Fig. 7** shows a flow chart of a method for reducing friction in a warranty registration process and warranty claiming process, in accordance with some embodiments consistent with the present disclosure.

[0054] Initially, a warranty shield database is populated with transaction data related to all the payment transactions between the retailer/manufacturer and the user **103**.

[0055] At block **702**, the warranty management system **101** may verify whether the MCC matches with the MCC of the merchant associated with the e-commerce portal **111**. If the MCC matches with the e-commerce portal **111**, then the user **103** is performing CNP transaction. The transaction may be authorized and routed to the warranty management system 101 via the network **113**. The network **113** may receive or fetch a MCC code contained in the authorization request and may authorize the transaction. Subsequently, the warranty management system **101**

may send push notification to the user device **107** and request the user **103** to confirm the purchase made as indicated at the block **704**. In response to the request, the user **103** may send confirmation of the purchase made on the e-commerce portal **111**. Further, the warranty management system **101** may verify whether the warranty has been updated or not as indicated in the block **706**. If the warranty is not updated on the warranty management system **101**, then the flow moves to the block **708** and the process may stop. If the warranty of the product is updated on the warranty management system **101**, then the flow moves to block **710**. At block **710** the warranty management system **101** may request product purchase details from the e-commerce portal **111**. For instance, the warranty management system **101** may make a HTTP call to the e-commerce portal **111** and requests for invoice, the customer support information and warranty information of the purchased product. At block **712**, the warranty management system **101** may connect to the OEM **115** and provide purchase details.

[0056] At block **714**, the warranty management system **101** may update the information and may send push notification to the user device **107** associated with the user **103** as indicated in the block **716**. The user **103** may use the received information to claim a warranty. The process may be stopped as indicated in the block **718**.

[0057] Similarly, if the warranty management system **101** verifies that the MCC does not match with the MCC of the e-commerce portal **111** at block **702**, then the warranty management system **101** may send push notification to the user device **107** as indicated in the block **720**. At block **722**, the warranty management system **101** may verify whether the warranty is updated or not for the purchased product. If not, then the flow moves to the block **708** and the process may be stopped.

[0058] If the warranty of the product is updated on the warranty management system **101**, then the warranty management system **101** may send push notification (e.g., in the form of a text or audio alert) to the user device **107** as indicated at the block **724**. The received push notification may trigger the user device **107** to capture the invoice, image of the product or serial number of the product. The user **103** may capture the purchase details and share all the captured details to the warranty management system **101**. At block **712**, the warranty management system **101** may connect to the OEM **115** and provide purchase details on the purchase made. Further, the operations as explained in the blocks 714-718 are performed.

ADVANTAGES OF THE PRSENT DISCLOSURE

[0059] In the present disclosure, a manufacturer may receive an early warning of faulty parts of designs or products. As a result, the manufacturer may estimate the cost of warranty claims and may receive useful information on the product modification.

[0060] The present disclosure performs data analysis on warranty and maintenance policy. Consequently, the present disclosure may predict future claims and warranty cost earlier.

[0061] The present disclosure provides a central platform for the manufacturers, retailers/merchants, and consumers to communicate. As a result, a positive relationship may be maintained between the consumers and manufacturers.

[0062] In the present disclosure, the manufacturer may avoid counterfeit parts. As a result, the defame of brand image can be avoided.

[0063] In the present disclosure, the manufacturer may receive additional revenue through extension warranty schemes.

[0064] The present disclosure may keep track of warranty claims and make consumers aware of their rights. The present disclosure helps consumers to track warranty, track reward point expiry and may track the timelines of warranty claims.

[0065] The present disclosure ensures replacements or repairs of purchased product by genuine manufacturers or dealers. As a result, the counterfeit products may be avoided.

[0066] The present disclosure provides one stop-shop to the consumers for all warranty management issues related to any product purchased.

[0067] The present disclosure optimizes the value chain. As a result, incentives may be provided to issuers and/or acquirers at the manufacturer, consumer and/or dealer end.

[0068] The present disclosure increases a brand loyalty, enhances customer satisfaction and provides a smart trusted solution for key players in the warranty claim life cycle.

General computer system:

[0069] **Fig. 8** illustrates a block diagram of an exemplary computer system for implementing embodiments consistent with the present disclosure.

[0070] In an embodiment, the computer system **800** may be used to implement the system. The computer system **800** may include a central processing unit ("CPU" or "processor") **802**. The processor **802** may include at least one data processor developing a common transaction database based on inputs received via a network interface **803** and communication network **809**. The processor **802** 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. The computer system **800** may correspond to the warranty management system **101** shown in the **Figs. 1a and 1b**.

[0071] The processor **802** may be disposed in communication with one or more Input/Output (I/O) devices (**810** and **811**) via I/O interface **801**. The I/O interface **801** employ communication protocols/methods such as, without limitation, audio, analog, digital, monoaural, Radio Corporation of America (RCA) connector, stereo, IEEE-1394 high speed serial bus, serial bus, Universal Serial Bus (USB), infrared, Personal System/2 (PS/2) port, Bbayonet Neill-Concelman (BNC) connector, coaxial, component, composite, Digital Visual Interface (DVI), High-Definition Multimedia Interface (HDMI), Radio Frequency (RF) antennas, S-Video, Video Graphics Array (VGA), IEEE 802.11b/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), Worldwide Interoperability for Microwave access (WiMax), or the like, etc.

[0072] Using the I/O interface **801**, the computer system **800** may communicate with one or more I/O devices such as input devices **810** and output devices **811**. For example, the input devices **810** 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 devices **811** 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.

[0073] In some embodiments, the processor **802** may be disposed in communication with a communication network **809** via a network interface **803**. The network interface **803** may communicate with the communication network **809**. The network interface **803** 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 **809** may include, without limitation, a direct interconnection, Local Area Network (LAN), Wide Area Network (WAN), wireless network (e.g., using Wireless Application Protocol), the Internet, etc. Using the network interface **803** and the communication network **809**, the computer system **800** may communicate with inputs and provides output. The network interface **803** may employ connection protocols include, but not limited to, 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 **809** may correspond to the network **113** shown in the **Figs. 1a and 1b**.

[0074] The communication network **809** includes, but is not limited to, a direct interconnection, 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 and such. The communication network **809** may either be a dedicated network or a shared network, which represents an association of the different types of networks that use a variety of protocols, for example, Hypertext Transfer Protocol (HTTP), Transmission Control Protocol/Internet Protocol (TCP/IP), Wireless Application Protocol (WAP), etc., to communicate with each other. Further, the communication network **809** may include a variety of network devices, including routers, bridges, servers, computing devices, storage devices, etc.

[0075] In some embodiments, the processor **802** may be disposed in communication with a memory **805** (e.g., RAM, ROM, etc. not shown in **Fig. 4**) via a storage interface **804**. The storage interface **804** may connect to memory **805** 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), fiber 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.

[0076] The memory **805** may store a collection of program or database components, including, without limitation, application **806**, an operating system **807**, etc. In some embodiments, computer system **800** may store user/application data, 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.

[0077] The operating system **807** may facilitate resource management and operation of the computer system 800. Examples of operating systems include, without limitation, Apple™ Macintosh ™ OS X™, UNIX™, Unix-like system distributions (e.g., Berkeley Software Distribution (BSD), FreeBSD™, Net BSD™, Open BSD™, etc.), Linux distributions (e.g., Red Hat™, Ubuntu™, K-Ubuntu™, etc.), International Business Machines (IBM™) OS/2™, Microsoft Windows™ (XP™, Vista/7/8, etc.), Apple iOS™, Google Android™, Blackberry™ operating system (OS), or the like.

[0078] In some embodiments, the computer system **800** may implement web browser **808** stored program components. Web browser **808** 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 408 may utilize facilities such as AJAX, DHTML, Adobe™ Flash, Javascript, Application Programming Interfaces (APIs), etc. In some embodiments, the computer system 800 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, Common Gateway Interface (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.

[0079] In some embodiments, the computer system **800** 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.

[0080] Furthermore, one or more computer-readable storage media may be utilized in implementing embodiments consistent with the present disclosure. A computer-readable storage medium refers to any type of physical memory on which information or data readable by a processor may be stored. Thus, a computer-readable storage medium may store instructions for execution by one or more processors, including instructions for causing the

processor(s) to perform steps or stages consistent with the embodiments described herein. The term “computer-readable medium” should be understood to include tangible items and exclude carrier waves and transient signals, i.e., be non-transitory. Examples include Random Access Memory (RAM), Read-Only Memory (ROM), volatile memory, non-volatile memory, hard drives, Compact Disc (CD) ROMs, DVDs, flash drives, disks, and any other known physical storage media.

[0081] The described operations may be implemented as a method, system or article of manufacture using standard programming and/or engineering techniques to produce software, firmware, hardware, or any combination thereof. The described operations may be implemented as code maintained in a “non-transitory computer readable medium”, where a processor may read and execute the code from the computer readable medium. The processor is at least one of a microprocessor and a processor capable of processing and executing the queries. A non-transitory computer readable medium may include media such as magnetic storage medium (e.g., hard disk drives, floppy disks, tape, etc.), optical storage (CD-ROMs, DVDs, optical disks, etc.), volatile and non-volatile memory devices (e.g., EEPROMs, ROMs, PROMs, RAMs, DRAMs, SRAMs, Flash Memory, firmware, programmable logic, etc.), etc. Further, non-transitory computer-readable media may include all computer-readable media except for a transitory. The code implementing the described operations may further be implemented in hardware logic (e.g., an integrated circuit chip, Programmable Gate Array (PGA), Application Specific Integrated Circuit (ASIC), etc.).

[0082] The illustrated steps are set out to explain the exemplary embodiments shown, and it should be anticipated that ongoing technological development will change the manner in which particular functions are performed. These examples are presented herein for purposes of illustration, and not limitation. Further, the boundaries of the functional building blocks have been arbitrarily defined herein for the convenience of the description. Alternative boundaries can be defined so long as the specified functions and relationships thereof are appropriately performed. Alternatives (including equivalents, extensions, variations, deviations, etc., of those described herein) will be apparent to persons skilled in the relevant art(s) based on the teachings contained herein. Such alternatives fall within the scope and spirit of the disclosed embodiments. It must also be noted that as used herein, the singular forms “a,” “an,” and “the” include plural references unless the context clearly dictates otherwise.

[0083] Furthermore, one or more computer-readable storage media may be utilized in implementing embodiments consistent with the present disclosure. A computer readable storage medium refers to any type of physical memory on which information or data readable by a processor may be stored. Thus, a computer readable storage medium may store instructions for execution by one or more processors, including instructions for causing the processor(s) to perform steps or stages consistent with the embodiments described herein. The term "computer readable medium" should be understood to include tangible items and exclude carrier waves and transient signals, i.e., are non-transitory. Examples include Random Access Memory (RAM), Read-Only Memory (ROM), volatile memory, non-volatile memory, hard drives, CD ROMs, DVDs, flash drives, disks, and any other known physical storage media.

[0084] 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. Accordingly, the disclosure of the embodiments of the disclosure is intended to be illustrative, but not limiting, of the scope of the disclosure.

[0085] With respect to the user of substantially any plural and/or singular terms herein, those having skill in the art can translate from the plural to the singular and/or from the singular to the plural as is appropriate to the context and/or application. The various singular/plural permutations may be expressly set forth herein for sake of clarity.

VISA WARRANTY SHIELD

ABSTRACT

The present disclosure relates to techniques for reducing the friction in warranty registration and warranty claim process using a warranty management system. The proposed warranty management system may communicate with merchant/retailer, user/customer and/or Original Equipment Manufacturer (OEM). Specifically, the user may purchase a product and initiate a transaction for the payment. The transaction may be authorized by a network and Merchant Category code may be fetched up by the network. The warranty management system may send notification to the user for requesting confirmation on the purchase. In response, the user may confirm the purchase of the product. Subsequently, the warranty management system may call e-commerce portal and request purchase details such as invoice, a customer support information, a warranty information etc. All the purchase details are retrieved by the user device associated with the user. Finally, the warranty management system may call OEM and provide all the details for the future access.

Fig. 1A

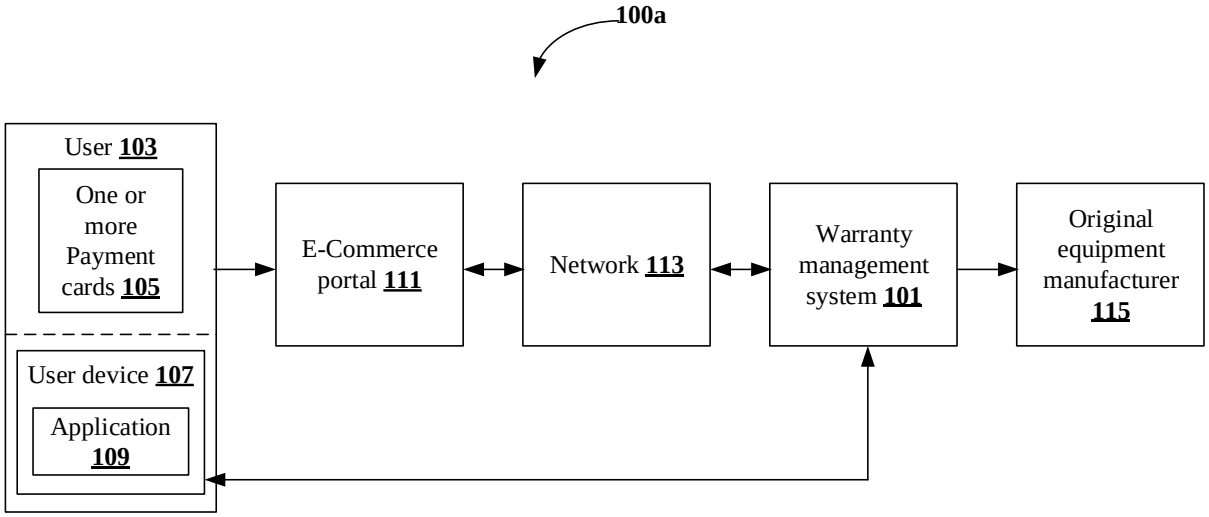
100a
User 103
One or more Payment cards 105
User device 107
Application 109
E-Commerce portal 111
Network 113
Warranty management system 101
Original equipment manufacturer 115

Fig. 1A

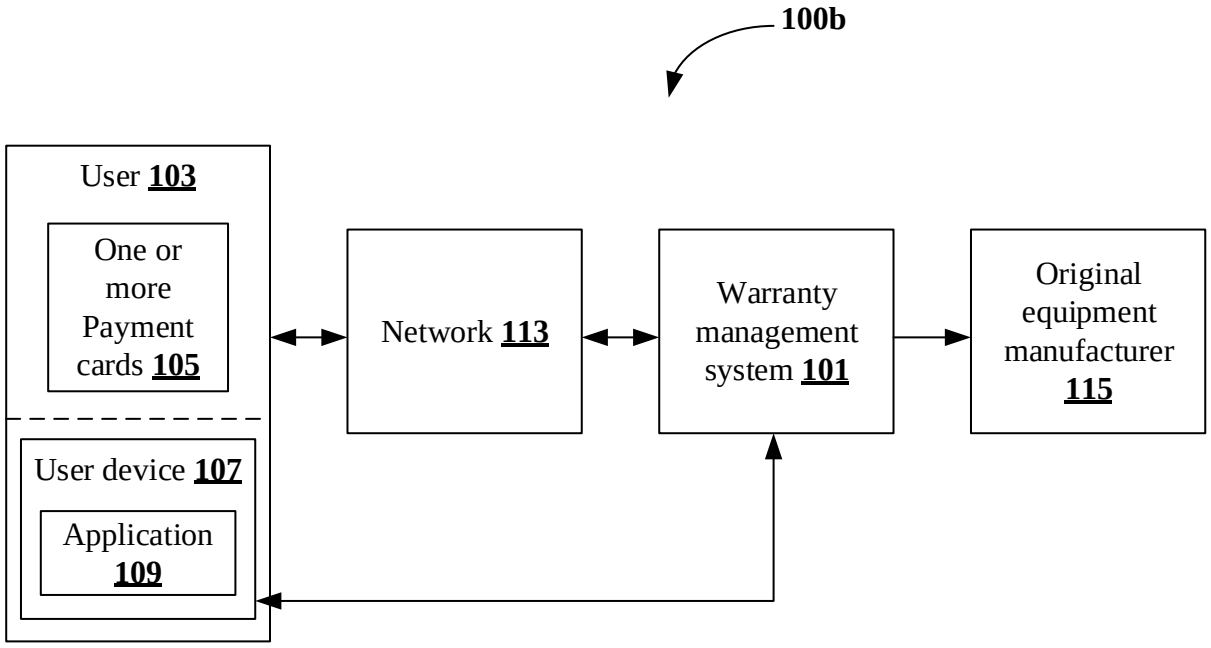
100b
User 103
One or more Payment cards 105
User device 107
Application 109
Network 113
Warranty management system 101
Original equipment manufacturer 115

Fig. 1B

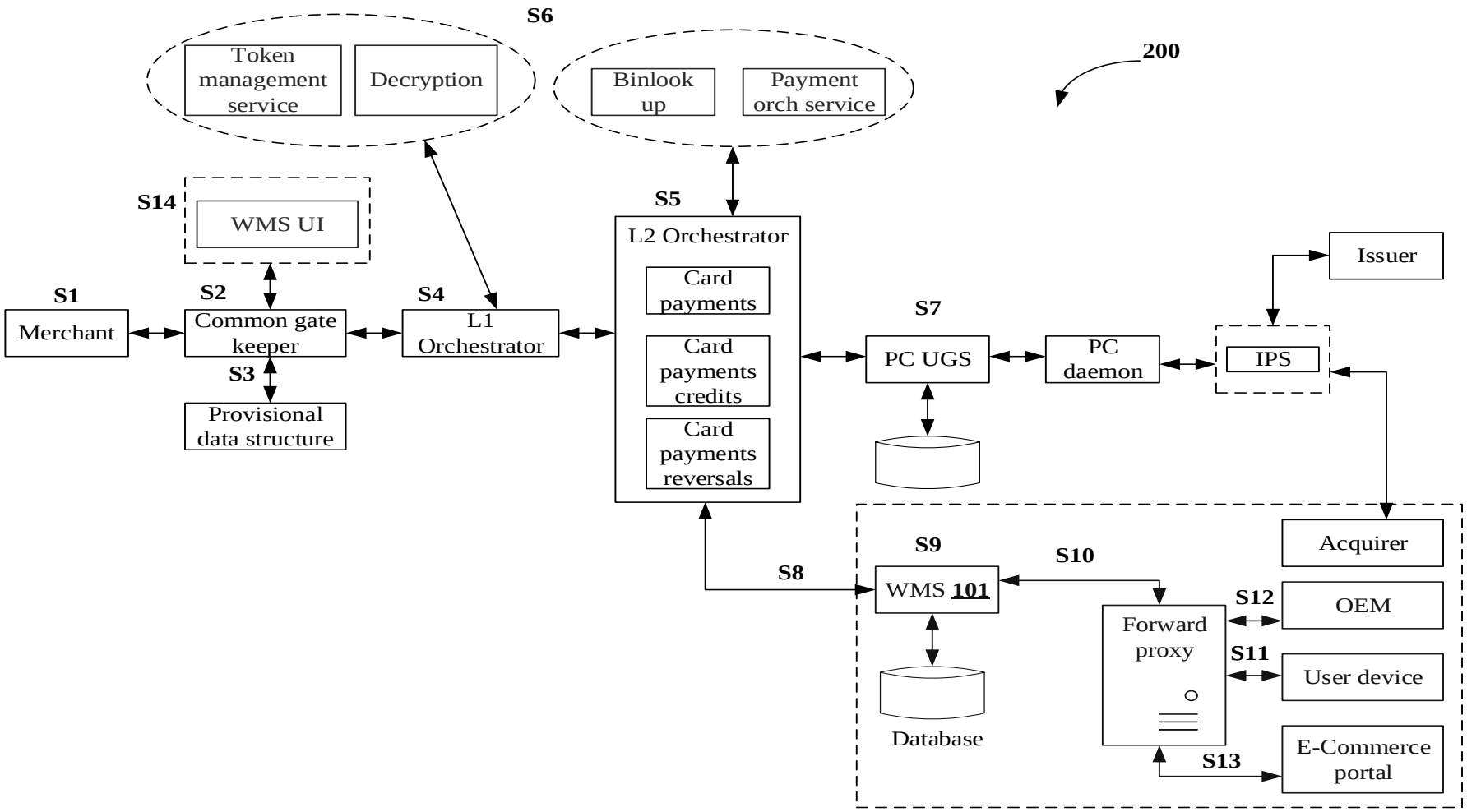
S6
Token management service
Decryption
Binlook up
Payment orch service
200
S14
WMS UI
S5
L2 Orchestrator
Card payments
Card payments credits
Card payments reversals
Issuer
S1
Merchant
S2
Common gate keeper
S3
Provisional data structure
S4
L1 Orchestrator
S7
PC UGS
PC daemon
IPS
S8
S9
WMS 101
S10
Database
Forward proxy
S12
OEM
S11
User device
S13
E-Commerce portal
Acquirer

Fig. 2

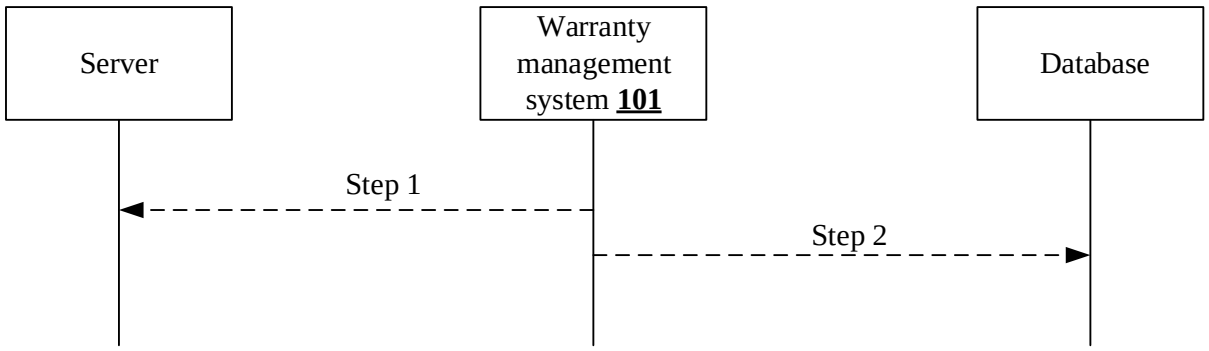

Fig. 3

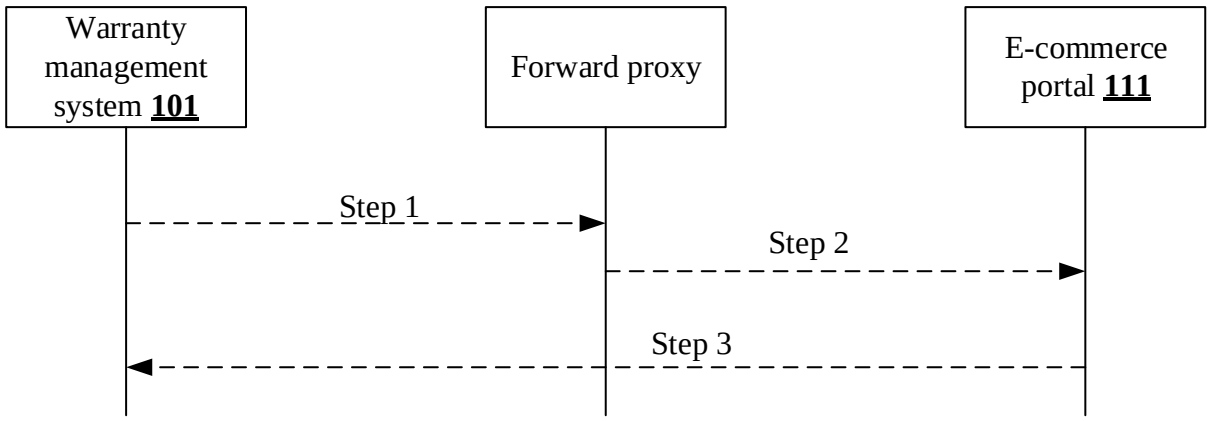

Fig. 4

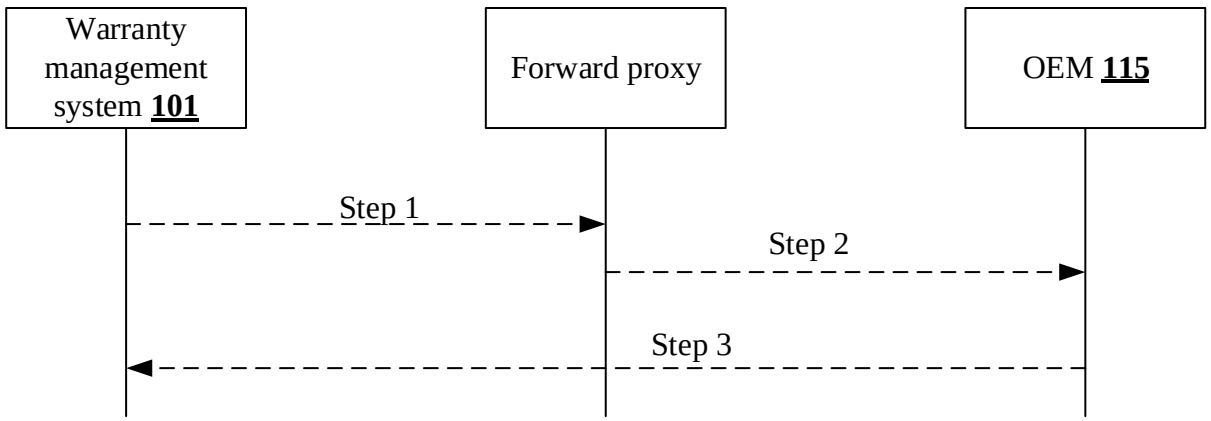

Fig. 5

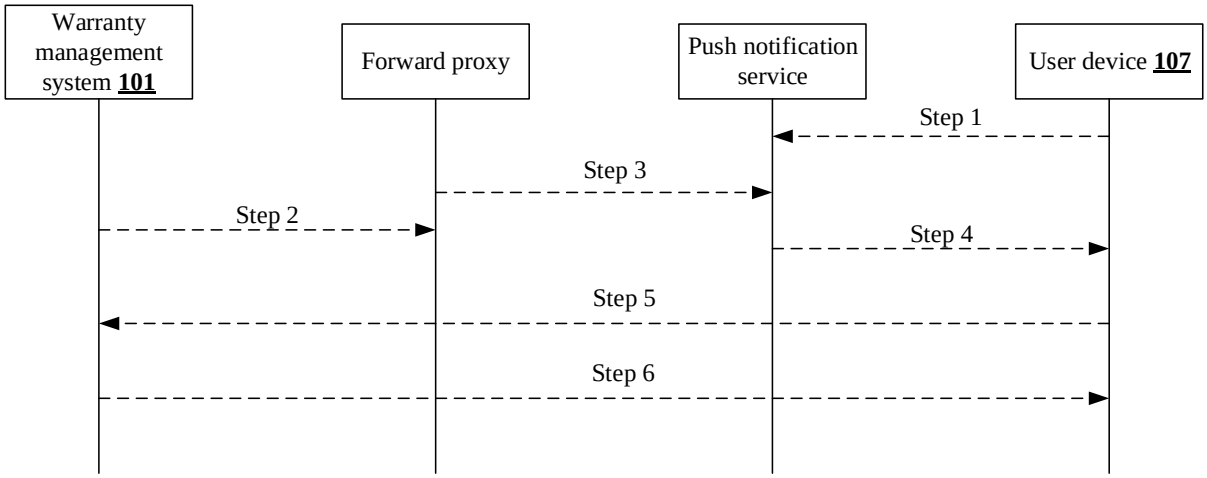
Warranty management system **101**
Forward proxy
Push notification service
User device **107**
Step 1
Step 3
Step 2
Step 4
Step 5
Step 6

Fig. 6

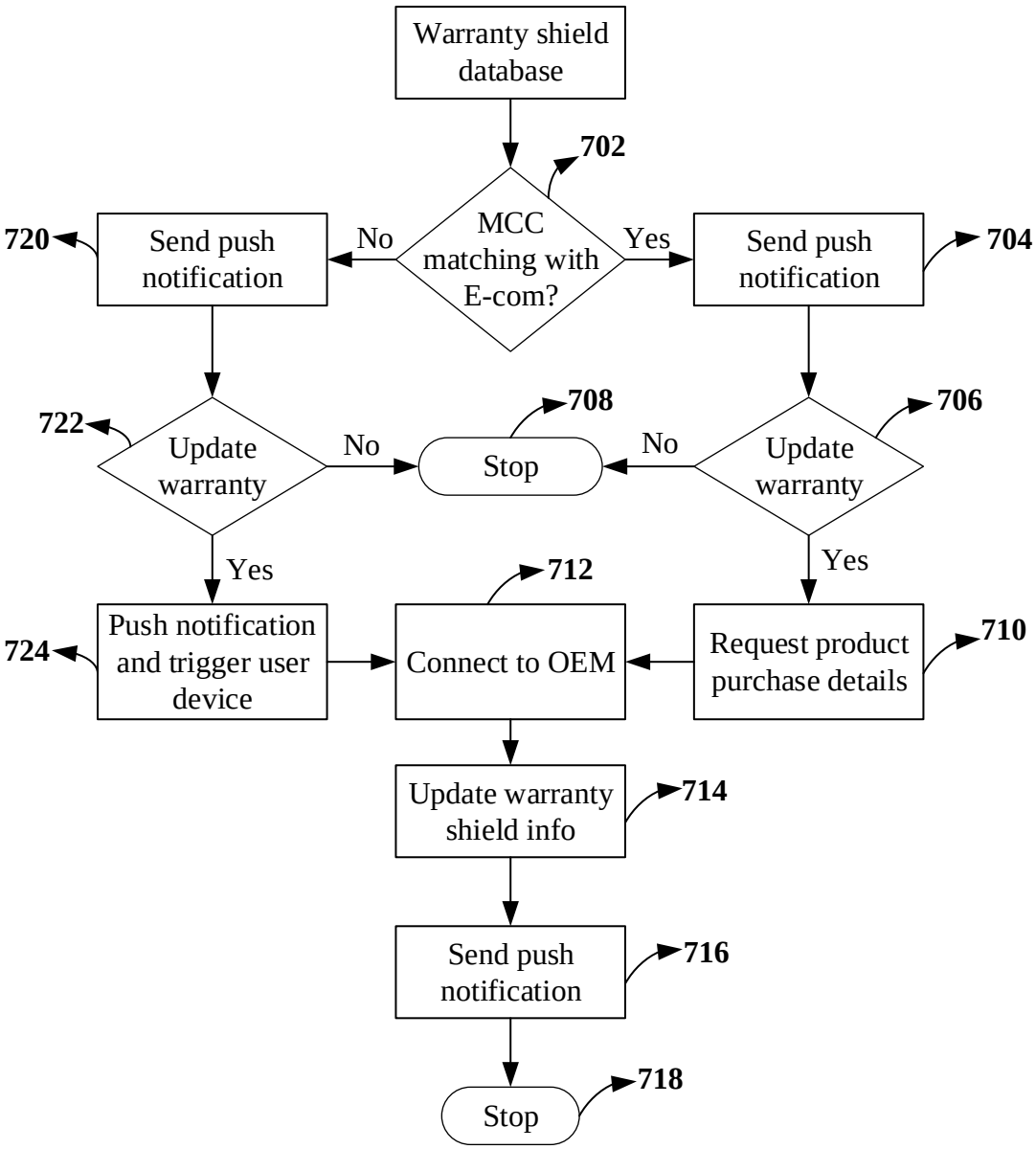
Warranty shield database
702
MCC matching with E-com?
No
Yes
720
Send push notification
Send push notification
704
722
Update warranty
No
708
Stop
No
706
Update warranty
Yes
Yes
712
724
Push notification and trigger user device
Connect to OEM
Request product purchase details
710
Update warranty shield info
714
Send push notification
716
Stop
718

Fig. 7

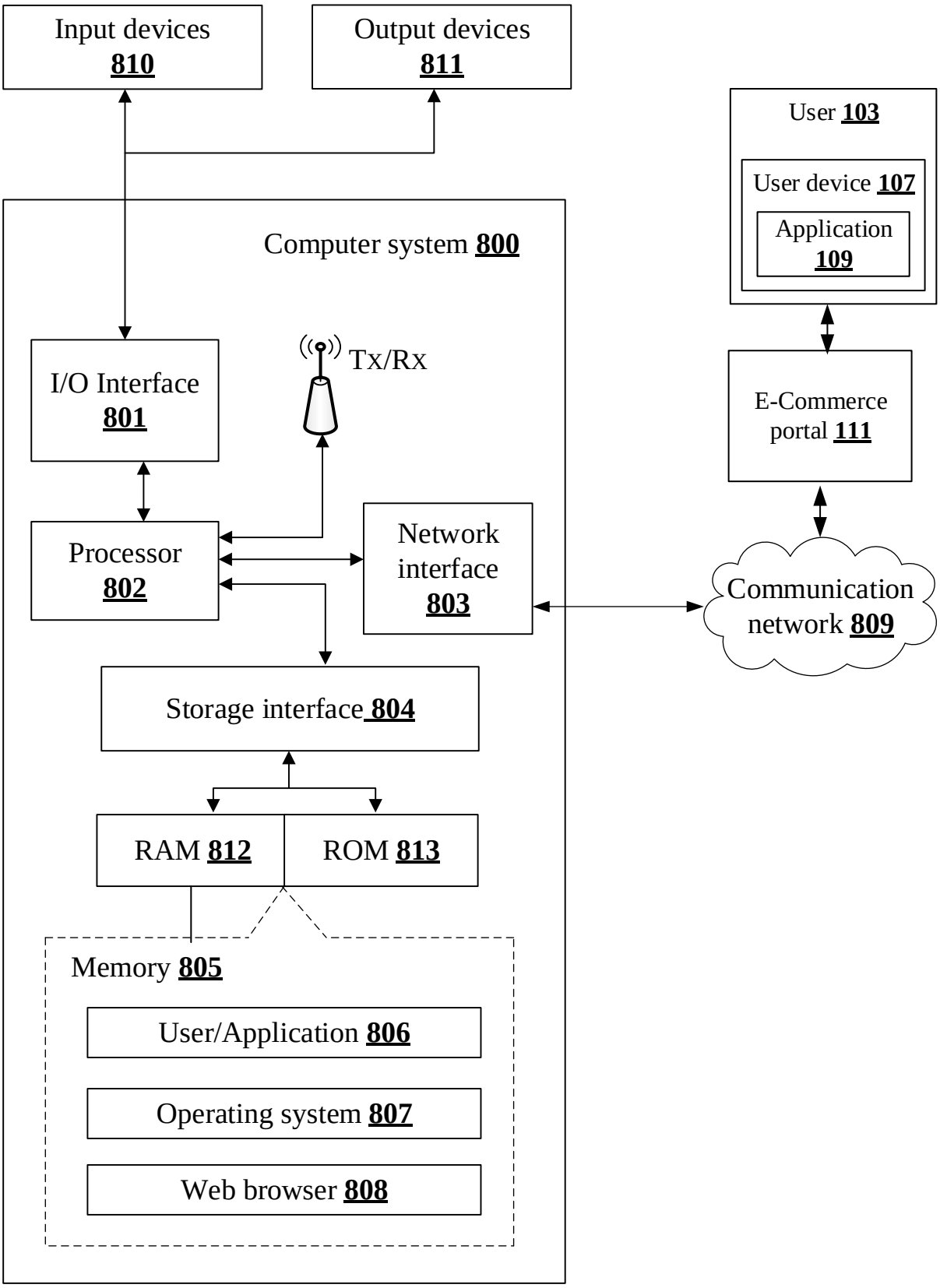
Input devices
810
Output devices
811
User 103
User device 107
Application
109
Computer system 800
I/O Interface
801
Tx/Rx
E-Commerce
portal 111
Processor
802
Network
interface
803
Communication
network 809
Storage interface 804
RAM 812
ROM 813
Memory 805
User/Application 806
Operating system 807
Web browser 808

Fig. 8