

from the cardholder information database. Then, the server determines if one of the trigger conditions for requiring execution of the MRAP is satisfied based on the information contained in the transaction request.

BRIEF DESCRIPTION OF THE DRAWINGS

[0011] Embodiments of the invention are illustrated by way of example and not by way of limitation in the figures of the accompanying drawings in which like references indicate similar elements. It should be noted that the references to “an embodiment” or “one embodiment” of this disclosure are not necessarily to the same embodiment, and such references mean at least one.

[0012] **FIG. 1** shows a block diagram of a system for performing secure online transactions according to an embodiment of the present invention.

[0013] **FIG. 2** shows a block diagram of a transaction authorization server coupled to a cardholder information database according to an embodiment of the present invention.

[0014] **FIG. 3** shows a flowchart diagram of a process for processing an online transaction request according to an embodiment of the present invention.

[0015] **FIG. 4** shows a flowchart diagram of a process for validating and analyzing reply messages received from mobile devices according to an embodiment of the present invention.

[0016] **FIG. 5** shows a flowchart diagram of a process for enabling selection of conditions for triggering an execution of a mobile reply authorization process according to an embodiment of the present invention.

DETAILED DESCRIPTION OF THE INVENTION

[0017] In the following description, specific details are set forth in order to provide a thorough understanding of various embodiments of the present invention. However, it will be apparent to one skilled in the art that embodiments of the present invention may be practiced without these specific details. In other instances, well-known hardware and software components, structures and techniques have not been shown in detail in order to avoid obscuring embodiments of the present invention.

[0018] Shown in **FIG. 1** is a simplified representation of a system **100** to facilitate secure sales transactions in accordance with an embodiment of the present invention. In this system, credit card users **102-1** through **102-N** can connect with an online merchant server **114** via a network **112** using their user computing devices **110-1** through **110-N**. The network **112** may include, for example, the Internet, a virtual private network (“VPN”), a wide area network (“WAN”) and/or a wireless network to enable data transmission between the user devices **110** and merchant server **114**. The user computing devices **110** can be any suitable device capable of establishing communication with the network, including personal computers, laptop computers, and/or wireless communications devices (e.g., cellular phones, personal digital assistants (“PDAs”)).

[0019] The merchant server **114** may be operated by a merchant offering various goods and/or services and may be

an application server, a web server or any other type of server capable of offering electronic commerce services over the Internet. A card user **102** may use Web browser software running on the user’s computing device to access and interact with Web pages **116** and other information provided by the merchant server **114** in which various types of goods and/or services are described and/or shown. To make a purchase, a card user **102** may provide the merchant **114** with transaction information required for conducting a transaction, such as, for example, the account number and expiration date of a transaction card. In one embodiment, the transaction card used is a credit or debit card having a non-secure magnetic stripe data memory.

[0020] The merchant server **114** may forward the transaction information provided by the card user and information about the purchase, such as price, item description and date of transaction to a payment server **118**. The payment server **118** may then generate a transaction request based on the transaction information received from the merchant server and forward the transaction request to a transaction processing system **120** that handles transactions for the specific transaction card. The system **120** processes the transaction request and returns an authorization granted or denied message to the payment server **119**. The payment server **119** forwards the message from the system **120** to the merchant server **114** and based on the message, the merchant server **114** may complete the purchase requested by the card user.

[0021] In an embodiment, the transaction processing system **120** is also configured to receive transaction requests from a transaction computer **119**. The transaction computer **119** may be any special purpose device capable of handling transactions, including but not limited to automatic teller machines (“ATMs”), point of sale (POS) terminals and credit card terminals.

[0022] Although only one merchant server **114**, only one payment server **118** and only one transaction computer **119** are illustrated in **FIG. 1**, it should be understood that any number of merchant servers, payment servers and transaction computers **119** may be coupled to the transaction processing system **120** to submit transaction requests and receive transaction approval or denial information. The communication between the payment server **118** and the system **120** may be established using any suitable communication means, such as the Internet, the public switched telephone network, dedicated communication lines, or a combination thereof. Similarly, the communication between the transaction computer **119** and the system **120** may be established using any suitable communication means, such as the Internet, the public switched telephone network, dedicated communication lines, or a combination thereof.

[0023] The transaction processing system **120** may be maintained and operated by a card provider, a bank, a financial institution or other types of institutions. The system **120** may include one or more servers coupled to one or more databases. In the illustrated embodiment, the system **120** includes a transaction authorization server **122** which is in communication to receive transaction requests. The server **122** enables a card provider to notify its cardholder of pending transaction requests so that unknown or fraudulent charges can be immediately identified. Additionally, the server **122** enables the card provider to obtain direct authorization from cardholders to ensure that the transaction requests are being made by the authorized cardholders.