October 2023

METHOD AND SYSTEM FOR DETECTING FRAUDULENT TRANSACTIONS THROUGH PAYMENT CARD

Mohan Kumar Sabapathy

Vijayraj Shanmugaraj

Vaishale Mahadevan

“METHOD AND SYSTEM FOR DETECTING FRAUDULENT TRANSACTIONS THROUGH PAYMENT CARD”

VISA

INVENTORS:

MOHAN KUMAR SABAPATHY

VIJAYRAJ SHANMUGARAJ

VAISHALE MAHADEVAN

TECHNICAL FIELD

[0001] The present subject matter is, in general, related to biometric authentication and fraud detection. Specifically, the subject matter relates to a method and system for detecting fraudulent transactions through payment card.

BACKGROUND

[0002] The financial industry is constantly evolving with advancements in technology, offering convenient methods of transactions for consumers. However, with these advancements, the risk of fraudulent activities, especially in card-present transactions, has also increased. Card-present transactions involve a person physically presenting the payment card (such as credit/debit card) at a point of sale (POS) terminal. Ensuring the authenticity of the cardholder in such scenarios is a critical challenge. Traditional methods of authenticity often rely on static information such as card numbers, and signatures, which may be forged or stolen by fraudsters. In addition, the traditional methods rely on location, device, pin code, or password-based authentication, which may be replicated by fraudsters with sufficient resources and historical data of the original cardholder.

[0003] Thus, there is a need for a method and a system to overcome the above-mentioned problems.

BRIEF DESCRIPTION OF THE DRAWINGS

[0004] 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:

[0005] **Fig. 1** illustrates an environment for detecting fraudulent transactions through a payment card, in accordance with an embodiment of the present disclosure;

[0006] **Fig. 2** illustrates a cross-sectional view of the payment card, in accordance with an embodiment of the present disclosure;

[0007] **Fig. 3** illustrates an electronic circuitry of the payment card, in accordance with an embodiment of the present disclosure;

[0008] **Fig. 4** illustrates a block diagram of a system for detecting fraudulent transactions through the payment card, in accordance with an embodiment of the present disclosure; and

[0009] **Fig. 5** illustrates a flow chart depicting a method for detecting fraudulent transactions through the payment card, in accordance with an embodiment of the present disclosure.

[0010] 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

[0011] It is to be understood that the present disclosure may assume various alternative variations and step sequences, except where expressly specified to the contrary. It is also to be understood that the specific devices and processes illustrated in the attached drawings and described in the following specification are simply exemplary and non-limiting embodiments or aspects. Hence, specific dimensions and other physical characteristics related to the embodiments or aspects disclosed herein are not to be considered as limiting.

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

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

[0014] The terms “comprise”, “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.

[0015] 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.

[0016] The terms “including”, “comprising”, “having” and variations thereof mean “including but not limited to” unless expressly specified otherwise.

[0017] The present disclosure addresses the above-mentioned challenges by providing a novel method and system for detecting fraudulent transactions through payment card. The system is configured to perform data collection including finger imprint patterns, pressure data, finger placement and the like of authentic card holder. The data is collected during legitimate transactions performed at point-of-sale (POS) terminal. The data of authentic card holder is then used to establish a baseline holding pattern for the authentic cardholder. Subsequently, during subsequent transactions at the POS terminal, the system collects real-time finger imprint and pressure data and compares with the established baseline holding pattern to detect fraudulent transactions. The system provides a high level of security, as finger imprint patterns are difficult to replicate or impersonate.

[0018] **Fig. 1** illustrates an environment 100 for detecting fraudulent transactions through a payment card 102, in accordance with an embodiment of the present disclosure. The environment 100 includes the payment card 102 of a card holder 106, a merchant 108 associated with a Point of Sale (POS) terminal 110, an issuer 114 associated with the card holder’s account 116, an acquirer 118 associated with a merchant’s account 120, a payment processor 112 and a system 122.

[0019] In an embodiment, the payment card 102 may be a debit card. In another embodiment, the payment card 102 may be a credit card. In yet another embodiment, the payment card 102 may be a prepaid card. It may be noted that the payment card 102 is not limited to the mentioned types of payment cards. The payment card 102 belongs to the card holder 106. In an embodiment, the card holder 106 is a legitimate user of the payment card 102. The payment card 102 includes a plurality of tactile sensors 104. The plurality of tactile sensors 104 may be configured to measure pressure or force when the card holder 106 holds the payment card 102. The plurality of tactile sensors 104 may be configured to obtain a set of data associated with card holding behavior of the card holder 106. In an embodiment, the set of data includes at least finger imprints of the card holder 106, card holding patterns of the card holder 106, and pressure data associated with pressure applied on the payment card 102 when the card holder 106 holds the card. The set of data is collected and stored in a smart chip of the payment card 102 (explained in detail in Fig. 2).

[0020] In one implementation, the payment card 102 is issued by an issuer 114. In an embodiment, the issuer 114 is a financial institution, such as a bank that has issued a debit card as a payment card 102 to the card holder 106. In another embodiment, the issuer 114 is a financial institution such as a credit card company that has issued a credit card as the payment card 102 to the cardholder 106. In general, the issuer 114 maintains card holder’s account 116 associated with the payment card 102.

[0021] The card holder 106 may initiate a purchase transaction at the merchant 108 using the payment card 102. In general, the merchant 108 is a business entity or an individual that offers products or services for sale. In an example, the merchant 108 is an entity that accepts the payment card 102 as a form of payment for the products or services being provided to the card holder 106. The merchant 108 accepts the payment card 102 using a Point of Sale (POS) terminal 110. In general, POS terminal is a device used by merchants to facilitate transactions at a point where a customer makes a purchase. In an embodiment, the POS terminal 110 acts as an interface between the merchant 108, the issuer 114, and the payment processor 112. In an example, the POS terminal 110 is a hardware device that includes at least a computer, a barcode scanner for scanning product or service code, a touch screen display, a keyboard for input, a receipt printer for providing transaction receipt, and a card reader for processing card payments. In another example, the POS terminal 110 may be a combination of hardware and

software that manages purchases of the card holder 106, accepts payments and provides receipts. The POS terminal 110 may be configured to receive the set of data associated with the card holding patterns of the card holder 106.

[0022] Further, the merchant 108 has a merchant account 120 at the acquirer 118. In general, an acquirer is a financial institution (such as bank) that establishes and maintains relationship with merchants to enable the merchants to accept electronic payments. In an example, when the card holder 106 makes a transaction, the acquirer 118 may be responsible for capturing and transmitting transaction data to the payment processor 112 for authorization and settling funds at the merchant's account 120. In an embodiment, the payment processor 112 may be associated with the system 122.

[0023] In an embodiment, the system 122 may be configured to interact with the payment card 102, the POS terminal 110, and the payment processor 112 for detection of fraudulent transactions. In an embodiment, the system 122 may be configured to collect the set of data from the payment card 102. In another embodiment, the system 122 may be configured to collect the set of data from the POS terminal 110. Further, the system 122 may be configured to forward the set of data to the payment processor 112. The set of data may be removed from the payment card 102 once the set of data is forwarded to the payment processor 112. The system 122 may not be a part of the environment 100. In an embodiment, the payment processor 112 directly receives the set of data from the POS terminal 110.

[0024] In an embodiment, the payment processor 112 may be configured to enable financial transactions upon authentication of the card holder 106. In an example, the payment processor 112 acts as a mediator between the issuer 114 and the acquirer 118. In an embodiment, the payment processor 112 may be a part of the system 122. The payment processor 112 includes a machine learning model 112a. The machine learning model 112a is pre-fed with historical data associated with the card holding patterns of the card holder 106. The historical data is pre-fed during legitimate transactions performed at the POS terminal 110. In an embodiment, a certain number of initial transactions of the payment card 102 may be dedicated as legitimate transactions to store card holding patterns of the card holder 106 for training the machine learning model 112a.

[0025] The machine learning model 112a is trained with the historical data to learn the card holding patterns of the card holder 106. The historical data is then utilized to determine a baseline holding pattern for the card holder 106 along with a threshold score. Further, the machine learning model 112a of the payment processor 112 receives the set of data obtained in real time, during transactions via the POS terminal 110. In an embodiment, the payment processor 112 may be configured to compare the set of data with the historical data using the machine learning model 112a. In another embodiment, the machine learning model 112a may be configured to compare the set of data with the historical data. The comparison is done to identify a change in the card holding pattern when the payment card 102 is presented at the POS terminal 110. Based on the comparison, the set of data is allocated a score. In an embodiment, the score is allocated using the machine learning model that is trained to recognise card holding patterns of the card holder 106 and detect anomalies. In an example, if real-time card holding pattern is closely matching card holding pattern of the historical data, the score for the real-time card holding pattern may be low. In another example, if real-time card holding pattern is different from card holding pattern of the historical data, the score for the real-time card holding pattern may be high. In addition, the score may be close to the threshold score. The score allocated to the set of data is compared with the threshold score of the historical data. In an example, if the score is above the threshold score, the transaction is detected as fraudulent. Further, based on the detected fraudulent transaction, the payment processor 112 may decline the payment card 102 and ends the transaction.

[0026] **Fig. 2** illustrates a cross-sectional view of the payment card 102, in accordance with an embodiment of the present disclosure. The payment card 102 includes the plurality of tactile sensors 104, a smart chip 202, a WI-FI 204, and a section 206. The payment card 102 includes a plurality of sections, whereas one of the sections 206 has been explained elaborately in Fig. 2 and Fig. 3. Each of the plurality of sections is similar to the section 206. In an embodiment, the plurality of tactile sensors 104 are embedded in the plurality of sections of the payment card 102. The plurality of tactile sensors 104 are configured to sense pressure on the payment card 102 when the card holder 106 holds the payment card 102. In an embodiment, the plurality of tactile sensors 104 includes an electronic circuitry (as shown in Fig. 3) in each section of the payment card 102.

[0027] Referring now to **Fig. 3**, an electronic circuitry 300 of the payment card 102 is illustrated, in accordance with an embodiment of the present disclosure. The electronic

circuitry 300 is present in each section 206 of the payment card 102. The electronic circuitry 300 includes a piezoelectric cell 302, an analog-to-digital converter 304, and an amplifier. When the card holder 106 applies pressure on the payment card 102, the piezoelectric cell 302 is activated in a section (206, as shown in Fig. 3) where pressure is applied. The piezoelectric cell 302 generates a voltage proportional to the pressure applied on the piezoelectric cell 302. The generated voltage is fed into the amplifier and the analog-to-digital converter 304 in order to convert the voltage caused by the pressure on the piezoelectric cell 302 into decimal values. The decimal values are stored into an array, which is then transmitted to the smart chip 202 of the payment card 102. The smart chip 202 includes a flash memory that stores the decimal values.

[0028] The electronic circuitry 300 functions using a power source. In an embodiment, the power source is a battery that may be integrated into the payment card 102. In an example, the power source may be a lithium coin battery (e.g., CR2025) that is pre-charged with sufficient power to last for a certain duration of time. In another embodiment, the power source may be a capacitive circuit that gets charged on exposure to an electromagnetic filed generated by the POS terminal 110.

[0029] **Fig. 4** illustrates a block diagram 400 of a system 122 for detecting fraudulent transactions through the payment card 102, in accordance with an embodiment of the present disclosure. The system 122 is linked with the payment processor 112 and the machine learning model 112a to detect fraudulent transactions through the payment card 102. The system 122 may enable the payment processor 112 to perform a set of actions for detection of fraudulent transactions as explained in Figs. 1-3.

[0030] The system 122 may comprise an I/O interface 402, a processor 406, and a memory 408. The memory 408 may be communicatively coupled to the processor 406. The processor 406 may be implemented as one or more microprocessors, microcomputers, microcontrollers, digital signal processors, central processing units, state machines, logic circuitries, and/or any devices that manipulate signals based on operational instructions. Among other capabilities, the processor 406 is configured to fetch and execute computer-readable instructions stored in the memory 408. The I/O interface 402 may include a variety of software and hardware interfaces, for example, a web interface, a graphical user interface, and the like. The I/O

interface 402 may enable the system 122 to communicate with other computing devices, such as web servers and external data servers (not shown).

[0031] **Fig. 5** illustrates a flow chart depicting a method 500 for detecting fraudulent transactions through the payment card 102, in accordance with an embodiment of the present disclosure.

[0032] The method 500 is explained in view of Figs. 1-4. The steps of the method 500 may be performed herein either by the processor 408 of the system 122, or the payment processor 112 or a combination thereof. To describe the method 500, the reference numerals are used in conjunction with Figs. 1-4. The method 500 starts at step 502.

[0033] At step 502, the method 500 includes collecting and storing the set of data. The set of data is collected upon activation of the plurality of tactile sensors 104. The set of data is stored in the smart chip 202 of the payment card 102. The plurality of tactile sensors 104 are activated when the card holder 106 holds the payment card 102 during real-time transactions. The set of data includes but may not be limited to at least finger imprints of the card holder 106, card holding patterns of the card holder 106, and pressure data associated with pressure applied on the payment card 102 when the card holder 106 holds the payment card 102.

[0034] At step 504, the method 500 includes transmitting the set of data from the smart chip 202 of the payment card 102 to the POS terminal 110. In an embodiment, the POS terminal 110 acts as an interface between the merchant 108, the issuer 114, and the payment processor 112 (as explained in detail in Fig. 1).

[0035] At step 506, the method 500 includes forwarding the set of data from the POS terminal 110 to the payment processor 112. The set of data may be removed from the payment card 102 once the set of data is forwarded to the payment processor 112. In an example, the payment processor 112 acts as a mediator between the issuer 114 and the acquirer 118. The payment processor 112 includes the machine learning model 112a. The machine learning model 112a is pre-fed with the historical data associated with the card holding patterns of the card holder 106. The historical data is pre-fed during legitimate transactions performed at the POS terminal 110. The historical data is then utilized to determine a baseline holding pattern for the card holder 106 along with a threshold score.

[0036] In an embodiment, the method 500 includes training of the machine learning model 112a with the historical data to learn the card holding patterns of the card holder 106. Further, the set of data obtained in real time, during transactions via the POS terminal 110, is received at the machine learning model 112a of the payment processor 112.

[0037] At step 508, the method 500 includes comparing the set of data with the historical data. The comparison is done to identify a change in the card holding pattern when the payment card 102 is presented at the POS terminal 110. Based on the comparison, the set of data is allocated a score. The score allocated to the set of data is compared with the threshold score of the historical data.

[0038] At step 510, the method 500 includes detecting fraudulent transactions based on the comparison. In an example, if the score is above the threshold score, the transaction is detected as fraudulent. Further, based on the detected fraudulent transaction, the payment processor 112 may decline the payment card 102 and ends the transaction.

[0039] The present invention has various advantages over the prior art. The present invention may be applied in various industries where card-present transactions occur, including but not limited to banking, retail, and hospitality. The present invention has the potential to significantly reduce frauds associated with payment cards and enhance security of in-person financial transactions.

[0040] It will be understood by those within the art that, in general, terms used herein, and are generally intended as “open” terms (e.g., the term “including” should be interpreted as “including but not limited to,” the term “having” should be interpreted as “having at least,” the term “includes” should be interpreted as “includes but is not limited to,” etc.). For example, as an aid to understanding, the detail description may contain usage of the introductory phrases “at least one” and “one or more” to introduce recitations. However, the use of such phrases should not be construed to imply that the introduction of a recitation by the indefinite articles “a” or “an” limits any particular part of description containing such introduced recitation to inventions containing only one such recitation, even when the introductory phrases “one or more” or “at least one” and indefinite articles such as “a” or “an” (e.g., “a” and/or “an” should typically be interpreted to mean “at least one” or “one or more”) are included in the recitations;

the same holds true for the use of definite articles used to introduce such recitations. In addition, even if a specific part of the introduced description recitation is explicitly recited, those skilled in the art will recognize that such recitation should typically be interpreted to mean at least the recited number (e.g., the bare recitation of "two recitations," without other modifiers, typically means at least two recitations or two or more recitations).

[0041] While various aspects and embodiments have been disclosed herein, other aspects and embodiments will be apparent to those skilled in the art. The various aspects and embodiments disclosed herein are for purposes of illustration and are not intended to be limiting, with the true scope and spirit being indicated by the following detailed description.

“METHOD AND SYSTEM FOR DETECTING FRAUDULENT TRANSACTIONS THROUGH PAYMENT CARD”

ABSTRACT

The aspect of the present disclosure relates to a method (500) and a system (122) for detecting fraudulent transactions through payment card (102). The method (500) initiates with collecting and storing a set of data associated with card holding patterns of a card holder (106) using a smart chip (202) of the payment card (102). The set of data is transmitted from a smart chip (202) to a POS terminal (110) and forwarded to a payment processor (112). The payment processor (112) compares the set of data with historical data to identify a change in the card holding pattern when the payment card (102) is presented at the POS terminal (110).

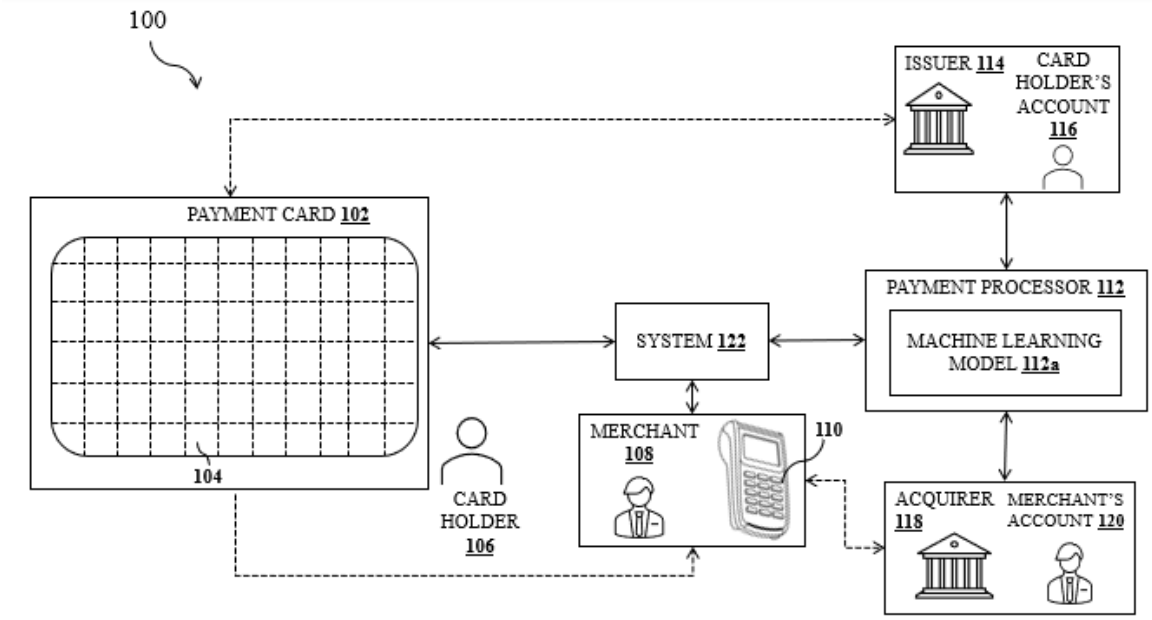
100
ISSUER 114
CARD HOLDER'S ACCOUNT 116
PAYMENT CARD 102
PAYMENT PROCESSOR 112
MACHINE LEARNING MODEL 112a
SYSTEM 122
MERCHANT 108
110
104
CARD HOLDER 106
ACQUIRER 118
MERCHANT'S ACCOUNT 120

FIGURE 1

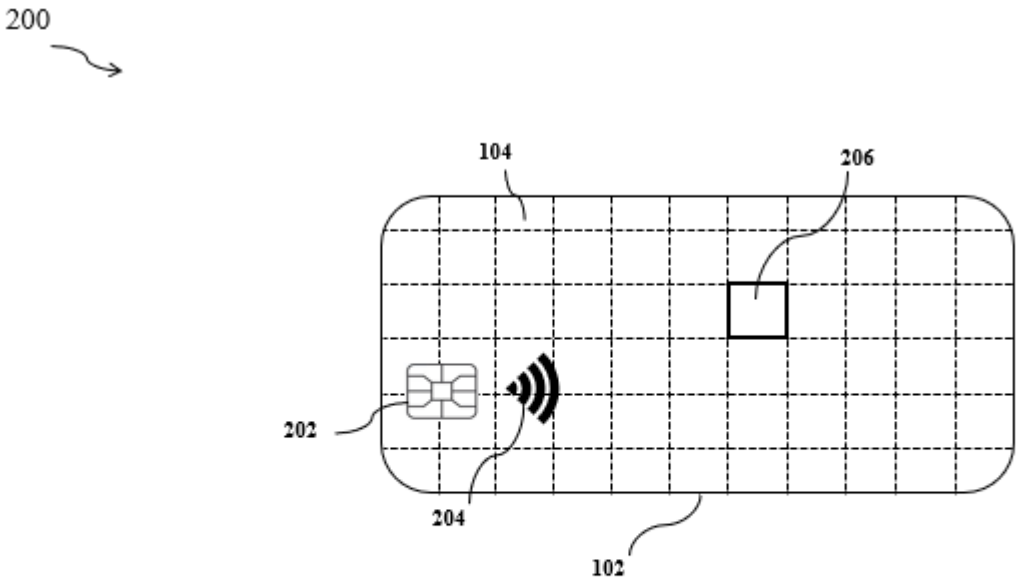

FIGURE 2

300

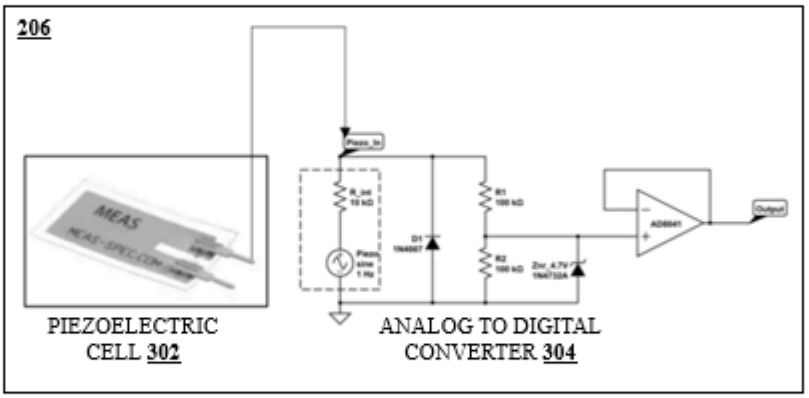
206
MEAS
PIEZOELECTRIC CELL 302
ANALOG TO DIGITAL CONVERTER 304

FIGURE 3

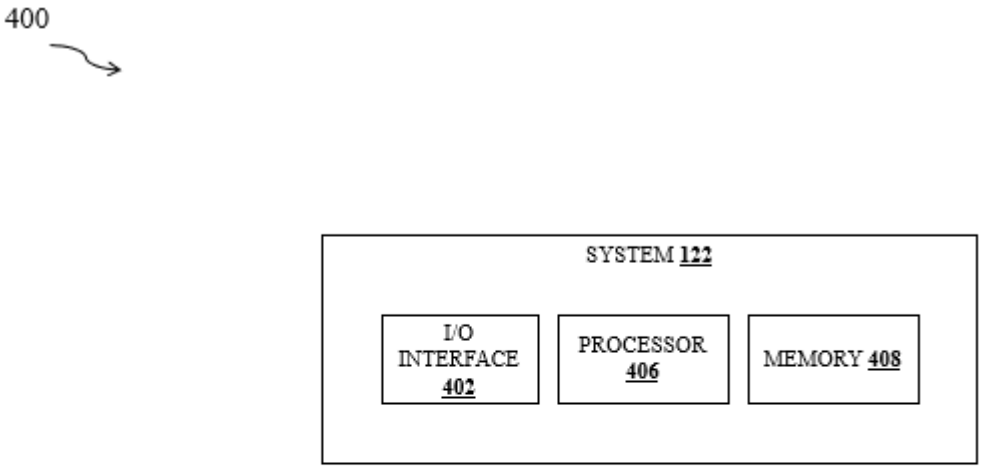

FIGURE 4

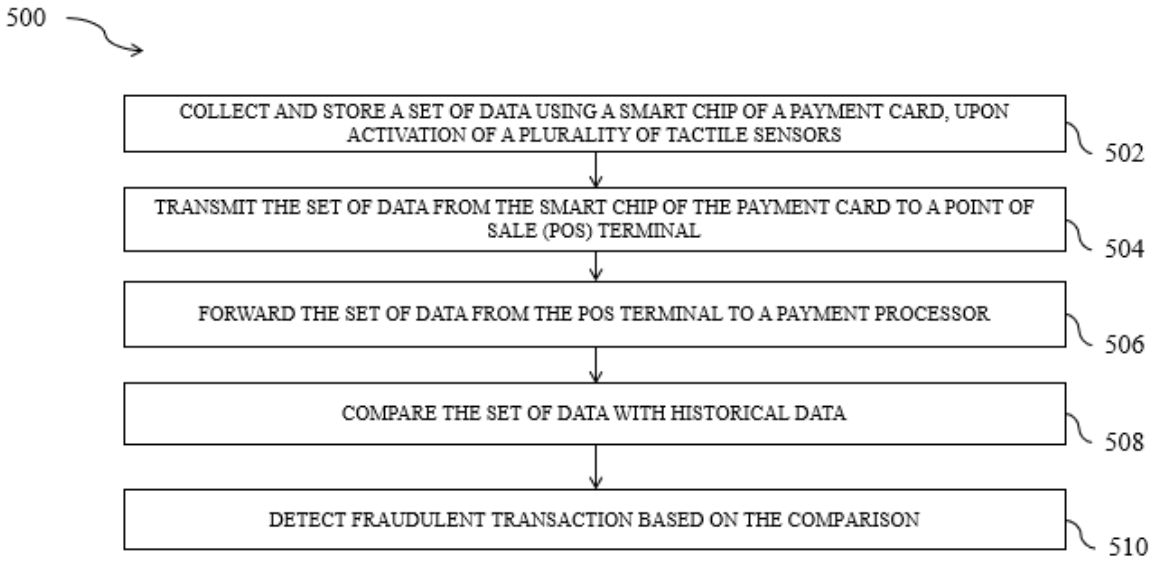
500
COLLECT AND STORE A SET OF DATA USING A SMART CHIP OF A PAYMENT CARD, UPON ACTIVATION OF A PLURALITY OF TACTILE SENSORS
502
TRANSMIT THE SET OF DATA FROM THE SMART CHIP OF THE PAYMENT CARD TO A POINT OF SALE (POS) TERMINAL
504
FORWARD THE SET OF DATA FROM THE POS TERMINAL TO A PAYMENT PROCESSOR
506
COMPARE THE SET OF DATA WITH HISTORICAL DATA
508
DETECT FRAUDULENT TRANSACTION BASED ON THE COMPARISON
510

FIGURE 5