August 2021

METHOD AND SYSTEM FOR ESTABLISHING CARDLESS ATM AUTHENTICATION AND VALIDATION USING FACE DETECTION

Cesar Otero
VISA

METHOD AND SYSTEM FOR ESTABLISHING CARDLESS ATM AUTHENTICATION AND VALIDATION USING FACE DETECTION

VISA

INVENTOR:
CESAR OTERO

TECHNICAL FIELD

[0001] This disclosure relates to card-less Automated Teller Machine (ATM) authentication and validation using face detection.

BACKGROUND

[0002] An Automated Teller Machine (ATM) card is a payment card or specialized payment card issued by a financial organisation for example a bank that allows a user to access their financial accounts. The use of ATM services is increasing day by day overseas and also it is associated with quite a few shortcomings. For example, losing an ATM card implies a cardholder losing access to ATM machines and their money. Especially when the user is traveling overseas it becomes more difficult as the user may not be able to replace their card immediately. Hence, one of the biggest challenges that users have is gaining access to ATM functions without using a physical ATM card or a phone.

BRIEF DESCRIPTION OF THE DRAWINGS

[0003] Additional advantages and details are explained in greater detail below with reference to the exemplary embodiments that are illustrated in the accompanying schematic figures, in which:

[0004] **Fig. 1** illustrates a block diagram of a system for implementing embodiments consistent with the present disclosure.

[0005] **Fig. 2** shows a flowchart illustrating a process for establishing card-less ATM authentication and validating using face detection.

[0006] **Fig. 3** illustrates a block diagram of an exemplary computer system for implementing embodiments consistent with the present disclosure.

DESCRIPTION OF THE DISCLOSURE

[0007] 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.

[0008] For purposes of the description hereinafter, the terms “end,” “upper,” “lower,” “right,” “left,” “vertical,” “horizontal,” “top,” “bottom,” “lateral,” “longitudinal,” and derivatives thereof shall relate to the disclosed subject matter as it is oriented in the drawing figures. However, it is to be understood that the disclosed subject matter 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 embodiments or aspects of the disclosed subject matter. Hence, specific dimensions and other physical characteristics related to the embodiments or aspects disclosed herein are not to be considered as limiting unless otherwise indicated.

[0009] No aspect, component, element, structure, act, step, function, instruction, and/or the like used herein should be construed as critical or essential unless explicitly described as such. Also, as used herein, the articles “a” and “an” are intended to include one or more items and may be used interchangeably with “one or more” and “at least one.” Furthermore, as used herein, the term “set” is intended to include one or more items (e.g., related items, unrelated items, a combination of related and unrelated items, and/or the like) and may be used interchangeably with “one or more” or “at least one.” Where only one item is intended, the term “one” or similar language is used. Also, as used herein, the terms “has,” “have,” “having,” or the like are intended to be open-ended terms. Further, the phrase “based on” is intended to mean “based at least partially on” unless explicitly stated otherwise.

[0010] It will be apparent that systems and/or methods, described herein, can be implemented in different forms of hardware, software, or a combination of hardware and software. The actual specialized control hardware or software code used to implement these systems and/or methods is not limiting of the implementations. Thus, the operation and behavior of the systems and/or methods are described herein without reference to specific software code, it being understood that software and hardware can be designed to implement the systems and/or methods based on the description herein.

[0011] Some non-limiting embodiments or aspects are described herein in connection with thresholds. As used herein, satisfying a threshold may refer to a value being greater than the threshold, more than the threshold, higher than the threshold, greater than or equal to the threshold, less than the threshold, fewer than the threshold, lower than the threshold, less than or equal to the threshold, equal to the threshold, etc.

[0012] **Fig.1** illustrates a block diagram of a system for implementing embodiments consistent with the present disclosure. The environment comprises a user 101, an ATM 103, and an authentication system [or system] 105. The system 105 may receive weather information 107 data from a device, where the device associated with the system 105 to determine the present weather status at the location. In an embodiment, the user 101 may choose to utilize an ATM 103 for cash withdrawal or other services while traveling overseas. Consider a scenario wherein the user 101 has lost his/her ATM card. In this situation, the present invention facilitates the user 101 to access ATM 103 functionality without the physical ATM card or a phone. At first, authentication of the user 101 is initiated by using ATM's 103 built-in Closed-Circuit Television (CCTV) camera for capturing an image of the user 101 along with the background details. Alternatively, any video capturing device embedded with the ATM 103 may be used for capturing the image of the user 101. The one or more parameters are used to authenticate the user 101. The one or more parameters including, but are not limited to, CCTV captured image, weather information 107 associated with the present location, geo-location of the current ATM 103 location, user 101 biometric data stored in the database, and motion detection. The CCTV captures the images during various weather conditions such as sunny, foggy, cloudy, mist, and rainy conditions.

[0013] In an embodiment, the system 105 receives the weather information 107 which has been collected from National Weather Service (NWS), wherein NWS is an open-source database which provides access to weather data and analysis of weather patterns. Initially, the system 105 determines the weather condition at user 101 location using retrieved data obtained from NWS such as sunny, foggy, rainy, mist, cloudy and so on.

The NWS provides weather data in JaveScript Object Notation (JSON) format or in any suitable format. Thereafter, the system 105 detects the weather condition from CCTV captured image and apply the Atmospheric Visibility method by using Convolution Neural Networks (CNN) based approach. CCN is adopted for extracting visibility features from the CCTV captured image. Further, the system 105 correlates the results obtained from NWS to results from CNN. Based on the correlation results, the system 105 assigns a score s1, wherein the score s1 may be one of high score or low score.

[0014] In an embodiment, the system 105 collects a geo-location information from the last ATM transaction performed by the user 101. Thereafter the system 105 compares the last known geo-location to the current ATM 103 geo-location, wherein the last know location are retrieved from call history stored in the server. The system 101 assigns a low score s2 unless the user 101 has traveled overseas tag or an ATM 103 located nearby, wherein the travel_tag is assigned when the user 101 traveled overseas. The history of user 101 geolocation is saved in an elastic search, wherein the elastic search is a distributed document store used to store complex data structures. Further, the system 105 compares the last known user 101 location with the current ATM 103 location using the logic defined as below:

[0015]

```
def compare_locations(travel_tag):
    current_location = atm location
    last = get_last_known() # retrieves in call to server
    distance = get_distance_difference(current_location, last)
    if !travel_tag:
        s2 = distance_score(distance)
    else:
        s2 = is_atm_in_travel_country(travel_tag)
    return s2
```

[0016] In an embodiment, a system 105 registers the user 101 biometric information with a picture being captured at the ATM 103. The CCTV captured image comprises the user’s biometric information, is forwarded to the server, wherein the biometric information includes the hair color of the user 101, skin color of the user 101, the distance between eyes of the user 101, facial shape, and the like. Thereafter the system 101 uses the captured CCTV image and measures the various characteristics of the user's face before converting it to a homomorphic hash, which is then saved in a key-value store database. Thereafter, the homomorphic hash is retrieved using a Permanent Account Number (PAN) as a key. The system 105 converts the CCTV captured image into a new hash and compares it with the hash number stored in a database. Further, the system 105 determines the identical hashes when compared with the hash number stored in the database and the result is stored as a score s3. The verification of the obtained biometric data using PAN is illustrated below:

[0017]

```
def check_biometrics(camera_input, pan): # use PAN to identify
        hash1 = convert_to_hash(camera_input)
        hash2 = get_hash(pan)
        s3 = hashes_match(hash1, hash2)
        return s3
```

[0018] The various biometric feature to homomorphic hash is as follows:

Distance between top of head and bottom of chin (f1)
Hair color (f2)
Skin color (f3)
Eye color (f4)
Distance between the centers of eye (f5)
Height of each ear (f6 and f7)
Distance between ears (f8)
Width and height of lips (f9 and f10)
homomorphic_hash_function applied to set of features [f1, f2, f3, f4, f5, f6, f7, f8, f9, f10]

[0019] In an embodiment, at first, a system 105 identifies the boundary of user 101 from the CCTV camera. Thereafter, the system 105 detects if there is any movement of the user 101 within the boundary. The system 105 verifies the CCTV image captured in front of the camera is a photograph or a real user 101 by using a motion detection, wherein the motion detection can be detected using OpenCV. OpenCV is an open-source computer vision library which is used in processing an image. By using OpenCV, system 105 may verify the boundary in the CCTV captured image. The system 105 detects the CCTV captured image is photograph held near camera by searching for borderlines of paper and then detects the border of user 101 faces.

[0020] Once the identification is completed, the system 105 then subtracts shadows from the image. Thereafter, the system 105 establishes a motion detection threshold which is appropriate and detects motion. Applying a differential of the background with the users face to detect motion is illustrated below:

diff = background - current_frame

[0021] If the differential exceeds a threshold level and there is no paper border, then the presence of user 101 is confirmed. Further, the system 105 stores the result of the motion detection as s4.

[0022] In an embodiment, the system 105 calculates the frequency of a fraudulent login attempt at authentication by using the probability image of the user 101 say P, where P (s1, s2, s3, s4). The system 105 receives the user 101 PIN after obtaining a high value of probability P and system 105 authenticated the user 101, wherein the value of P is based on the threshold value.

[0023] **Fig. 2** shows a flowchart illustrating a process for establishing card-less ATM authentication and validating using face detection. **At block 201**, the method comprises capturing an image of a user 101 using a built-in ATM's 103 CCTV camera. **At block 203**, the method comprises determining the weather condition at the current location, wherein the weather condition is obtained from NWS. Thereafter, the method determines the weather condition at user 101 location using retrieved data obtained from NWS such as sunny, foggy, rainy, mist, cloudy, and so on and detects the weather status from CCTV captured image. **At block 205**, the method comprises comparing the previous ATM usage location with the current ATM 103 location. **At block 207**, the method comprises comparing CCTV capture image with the user 101 data stored in the database. The CCTV captured image comprises the user's biometric information, is forwarded to the server. Further, converts the CCTV captured image into a new hash and compares it with the hash number stored in a database. **At block 209**, the method comprises verifying the movements by using motion detection and based on the highest probability values, user 101 is prompted to enter the PIN number. The motion detection verifies the movement of the user 101 in the image captured by the CCTV camera. **At block 211**, access to cash and other possible services upon user PIN authentication. In an embodiment, the present invention facilitates the user 101 to access ATM 103 functionality without the physical ATM card or a phone.

[0024] Computer System

[0025] **Fig. 3** illustrates a block diagram of an exemplary computer system for implementing embodiments consistent with the present disclosure.

[0026] In an embodiment, the computer system 300 may be used to implement the system. The computer system 300 may include a central processing unit (“CPU” or “processor”) 302. The processor 302 may include at least one data processor for performing accessible data visualization on a web platform. The processor 302 may include specialized processing units such as, integrated system (bus) controllers, memory management control units, floating point units, graphics processing units, digital signal processing units, etc.

[0027] The processor 302 may be disposed in communication with one or more input/output (I/O) devices (312 and 313) via I/O interface 301. The I/O interface 301 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, bayonet 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.

[0028] Using the I/O interface 301, the computer system 300 may communicate with one or more I/O devices such as input devices 312 and output devices 313. For example, the input devices 312 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 313 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.

[0029] In some embodiments, the processor 302 may be disposed in communication with a communication network 309 via a network interface 303. The network interface 303 may communicate with the communication network 309. The network interface 303 may employ connection protocols including, without limitation, direct connect, ethernet (e.g., twisted pair 10/100/1000 Base T), transmission control protocol/internet protocol (TCP/IP), token ring, IEEE 802.11a/b/g/n/x, etc. The communication network 309 may include, without limitation, a direct interconnection, local area network (LAN), wide area network (WAN), wireless network (e.g., using Wireless Application Protocol), the Internet, etc. Using the network interface 303 and the communication network 309, the computer system 300 may communicate with a database 314, which may be the enrolled templates database 313. The network interface 303 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.

[0030] The communication network 309 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 309 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 309 may include a variety of network devices, including routers, bridges, servers, computing devices, storage devices, etc.

[0031] In some embodiments, the processor 302 may be disposed in communication with a memory 305 (e.g., RAM, ROM, etc. not shown in FIGURE 3) via a storage interface 304. The storage interface 304 may connect to memory 305 including, without limitation, memory drives, removable disc drives, etc., employing connection protocols such as, serial advanced technology attachment (SATA), integrated drive electronics (IDE), IEEE-1394, universal serial bus (USB), 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.

[0032] The memory 305 may store a collection of program or database components, including, without limitation, user interface 306, an operating system 307, etc. In some embodiments, computer system 300 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.

[0033] The operating system 307 may facilitate resource management and operation of the computer system 300. Examples of operating systems include, without limitation, Apple^{TM} Macintosh ^{TM} OS X^{TM}, UNIX^{TM}, Unix-like system distributions (e.g., Berkeley Software Distribution (BSD), FreeBSD^{TM}, Net BSD^{TM}, Open BSD^{TM}, etc.), Linux distributions (e.g., Red Hat^{TM}, Ubuntu^{TM}, K-Ubuntu^{TM}, etc.), International Business Machines (IBM^{TM}) OS/2^{TM}, Microsoft Windows^{TM} (XP^{TM}, Vista/7/8, etc.), Apple iOS^{TM}, Google Android^{TM}, Blackberry^{TM} operating system (OS), or the like. In some embodiments, the computer system 300 may implement web browser 308 stored program components. Web browser 308 may be a hypertext viewing application, such as Microsoft^{TM} Internet Explorer^{TM}, Google Chrome^{TM}, Mozilla Firefox^{TM}, Apple^{TM} Safari^{TM}, etc. Secure web browsing may be provided using secure hypertext transport protocol (HTTPS), secure sockets layer (SSL), transport layer security (TLS), etc. Web browsers 308 may utilize facilities such as AJAX, DHTML, Adobe^{TM} Flash, Javascript, Application Programming Interfaces (APIs), etc.

[0034] According to some non-limiting embodiments or aspects, a computer program product including at least one non-transitory computer-readable medium including one or more instructions.

[0035] 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. Also, the words "comprising," "having," "containing," and "including," and other similar forms are intended to be equivalent in meaning and be open ended in that an item or items following any one of these words is not meant to be an exhaustive listing of such item or items, or meant to be limited to only the listed item or items. 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.

[0036] 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.

[0037] 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.

METHOD AND SYSTEM FOR CARDLESS ATM AUTHENTICATION AND VALIDATION USING FACE DETECTION

ABSTRACT

The present disclosure relates to a method and system for card-less Automated Teller Machine (ATM) authentication and validation using face detection. The cardholder's image is captured using the ATM's built-in cameras. Determine the weather condition at the present location obtained from National Weather Services and correlate with the CCTV captured image. Thereafter compare the CCTV captured image with the user data stored in a database. Further, verify the user movements by using a motion detection method, and based on verification, user is prompted to enter a PIN number to authenticate the transaction. Based on the PIN number authentication, the user is allowed to access cash or other possible services. Allowing card-less/phoneless ATM transactions assist the user to get access to their money even if they have misplaced their cards, phone, or wallet.

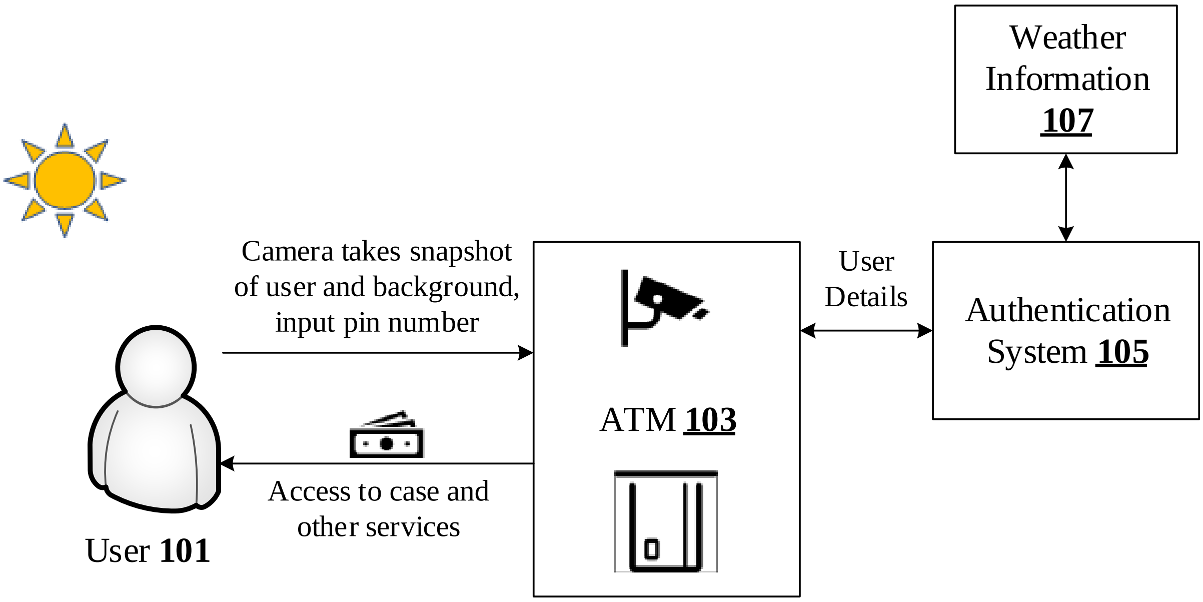
Weather Information 107
Camera takes snapshot of user and background, input pin number
User Details
Authentication System 105
ATM 103
User 101
Access to case and other services

Fig. 1

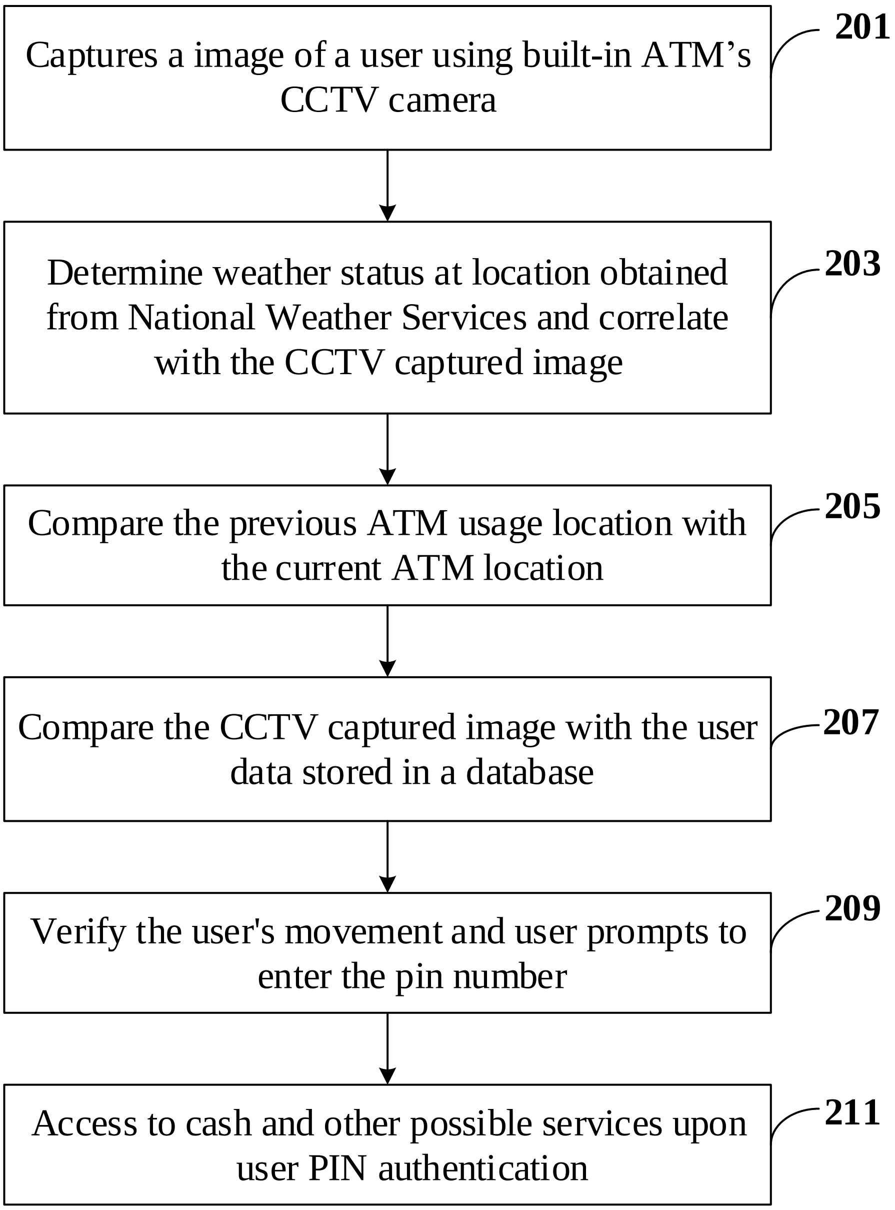
Captures a image of a user using built-in ATM’s CCTV camera
201
Determine weather status at location obtained from National Weather Services and correlate with the CCTV captured image
203
Compare the previous ATM usage location with the current ATM location
205
Compare the CCTV captured image with the user data stored in a database
207
Verify the user's movement and user prompts to enter the pin number
209
Access to cash and other possible services upon user PIN authentication
211

Fig. 2

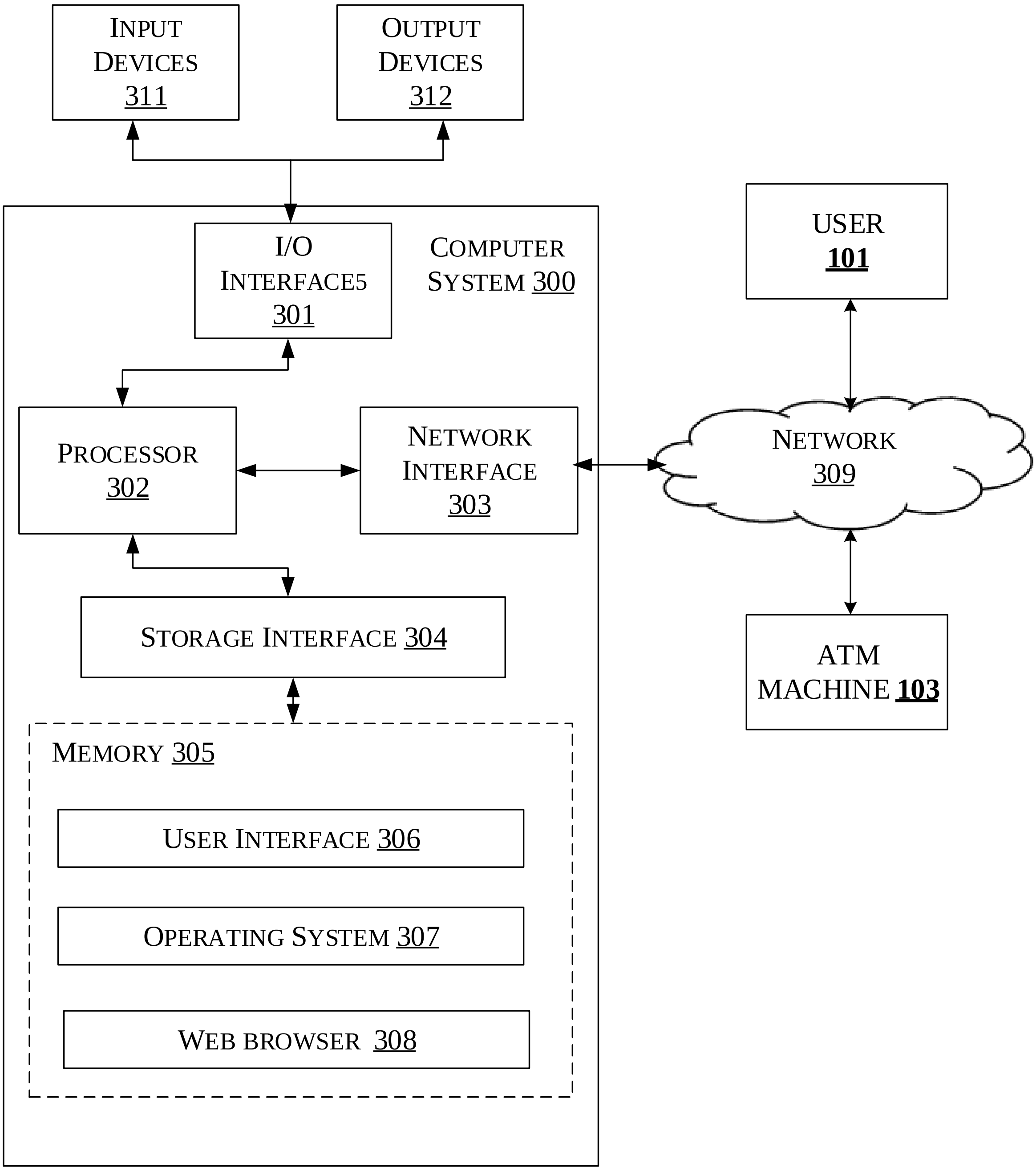
INPUT DEVICES 311
OUTPUT DEVICES 312
I/O INTERFACE5 301
COMPUTER SYSTEM 300
USER 101
PROCESSOR 302
NETWORK INTERFACE 303
NETWORK 309
STORAGE INTERFACE 304
ATM MACHINE 103
MEMORY 305
USER INTERFACE 306
OPERATING SYSTEM 307
WEB BROWSER 308

Fig. 3