US 20110138450A1

(19) United States

(12) Patent Application Publication

Kesanupalli et al.

(10) Pub. No.: US 2011/0138450 A1

(43) Pub. Date: Jun. 9, 2011

(54) **SECURE TRANSACTION SYSTEMS AND METHODS USING USER AUTHENTICATING BIOMETRIC INFORMATION**

(75) Inventors: **Ramesh Kesanupalli**, San Jose, CA (US); **Davit Baghdasaryan**, Fremont, CA (US); **Frank Schwab**, Phoenix, AZ (US); **Philip Yiu Kwong Chan**, Fremont, CA (US); **Larry Hattery**, Beaverton, OR (US)

(73) Assignee: **Validity Sensors, Inc.**, San Jose, CA (US)

(21) Appl. No.: **12/793,499**

(22) Filed: **Jun. 3, 2010**

Related U.S. Application Data

(60) Provisional application No. 61/249,218, filed on Oct. 6, 2009, provisional application No. 61/292,820, filed on Jan. 6, 2010.

Publication Classification

(51) **Int. Cl.**

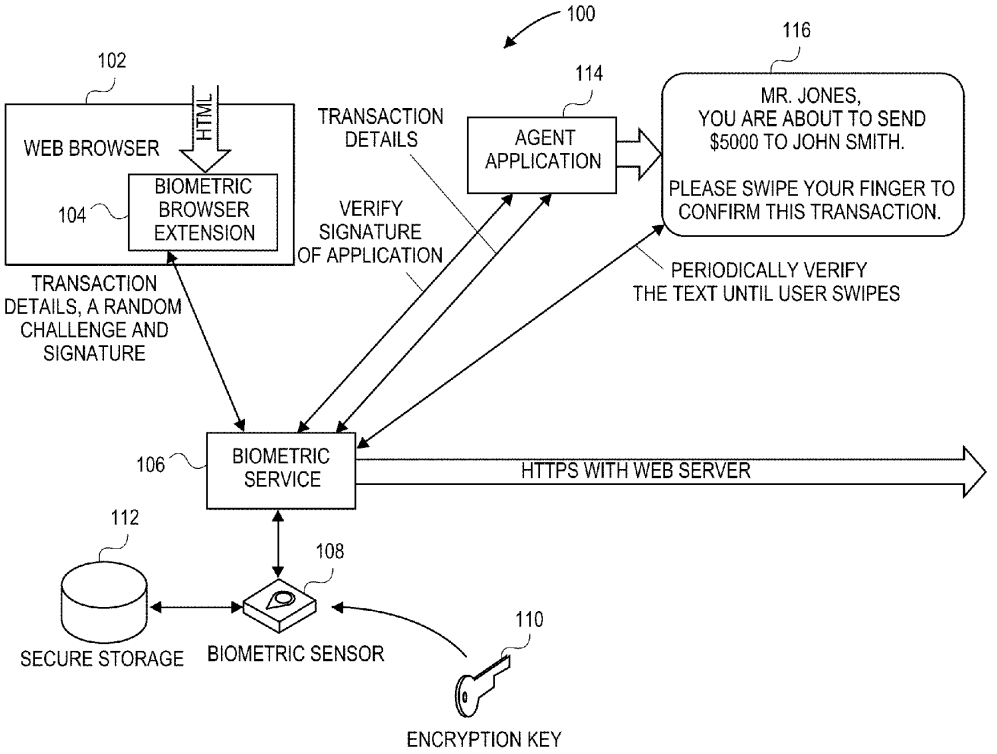
H04L 9/32 (2006.01)

G06F 21/00 (2006.01)

(52) **U.S. Cl.** **726/7**

(57) **ABSTRACT**

A user transaction request is received at a client device. A web browser plug-in communicates the user transaction request to a server that determines whether the user transaction request is a secure transaction. Transaction data is received from the server via the web browser plug-in. If the received transaction data indicates a secure transaction, the user is prompted to provide biometric data from a user using a biometric device and related security protocols. The web browser plug-in then communicates a transaction confirmation to the server.



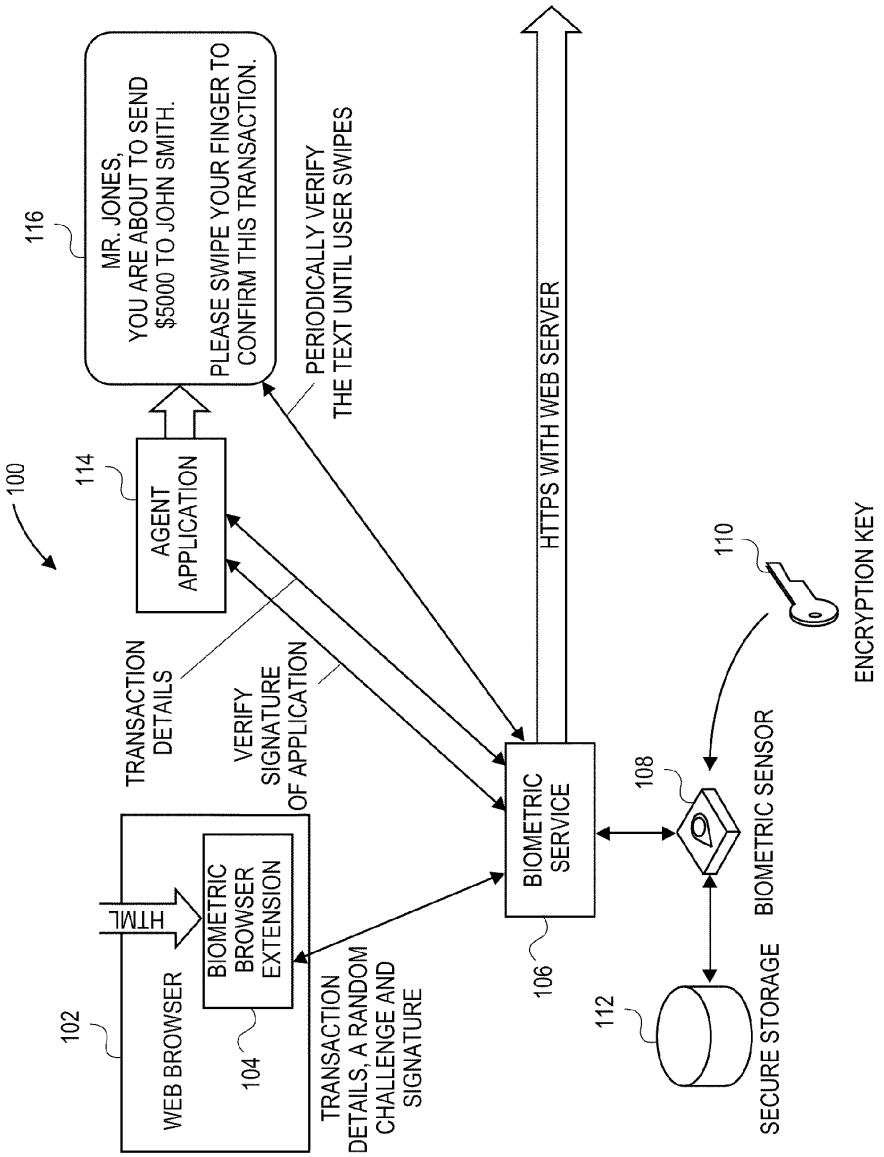

100
116
MR. JONES,
YOU ARE ABOUT TO SEND
$5000 TO JOHN SMITH.
PLEASE SWIPE YOUR FINGER TO
CONFIRM THIS TRANSACTION.
114
AGENT
APPLICATION
PERIODICALLY VERIFY
THE TEXT UNTIL USER SWIPES
HTTPS WITH WEB SERVER
TRANSACTION
DETAILS
VERIFY
SIGNATURE
OF APPLICATION
110
ENCRYPTION KEY
HTML
BIOMETRIC
BROWSER
EXTENSION
BIOMETRIC
SERVICE
108
BIOMETRIC SENSOR
102
WEB BROWSER
104
TRANSACTION
DETAILS, A RANDOM
CHALLENGE AND
SIGNATURE
106
112
SECURE STORAGE

FIG. 1

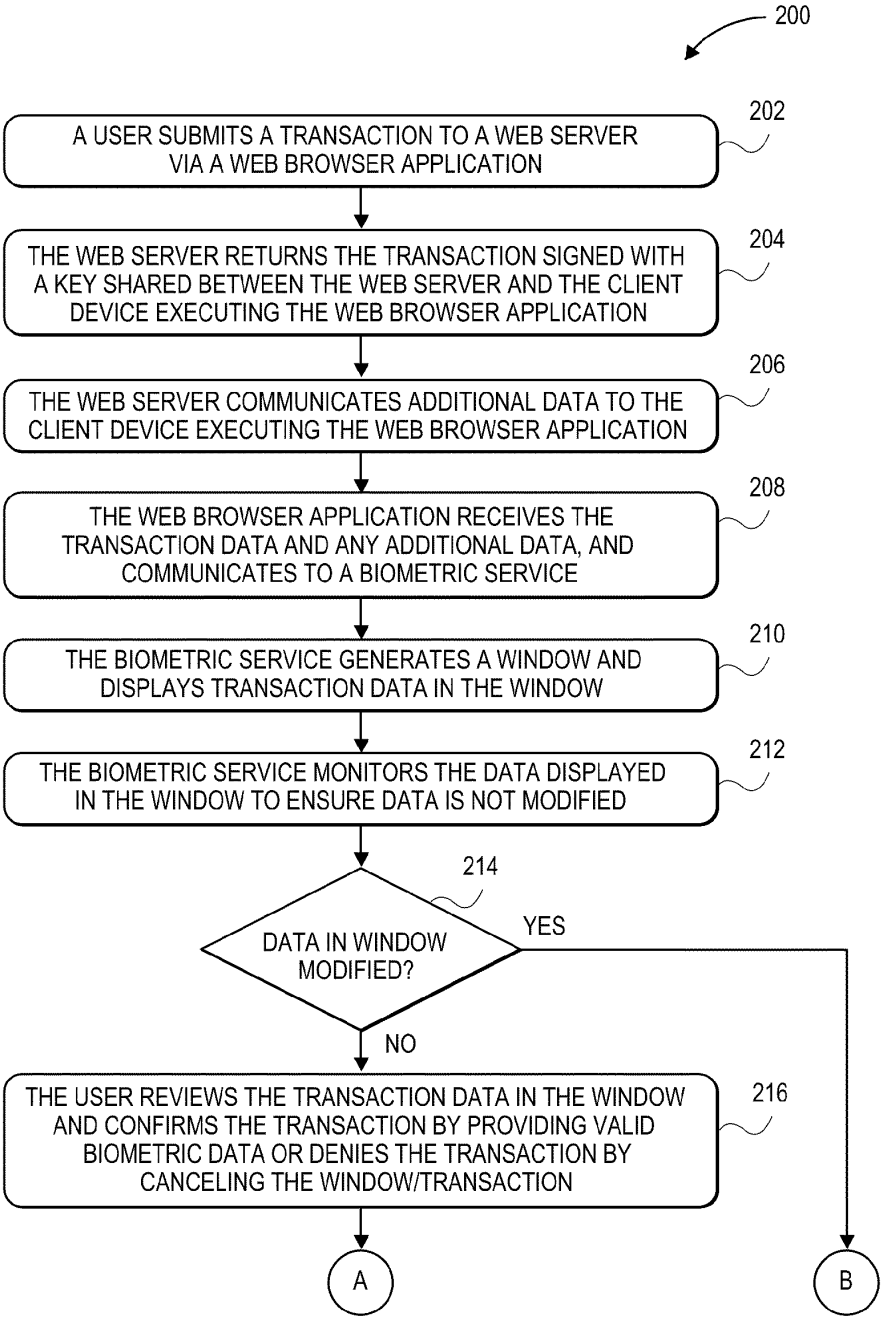

200
202
A USER SUBMITS A TRANSACTION TO A WEB SERVER VIA A WEB BROWSER APPLICATION
204
THE WEB SERVER RETURNS THE TRANSACTION SIGNED WITH A KEY SHARED BETWEEN THE WEB SERVER AND THE CLIENT DEVICE EXECUTING THE WEB BROWSER APPLICATION
206
THE WEB SERVER COMMUNICATES ADDITIONAL DATA TO THE CLIENT DEVICE EXECUTING THE WEB BROWSER APPLICATION
208
THE WEB BROWSER APPLICATION RECEIVES THE TRANSACTION DATA AND ANY ADDITIONAL DATA, AND COMMUNICATES TO A BIOMETRIC SERVICE
210
THE BIOMETRIC SERVICE GENERATES A WINDOW AND DISPLAYS TRANSACTION DATA IN THE WINDOW
212
THE BIOMETRIC SERVICE MONITORS THE DATA DISPLAYED IN THE WINDOW TO ENSURE DATA IS NOT MODIFIED
214
DATA IN WINDOW MODIFIED?
YES
NO
216
THE USER REVIEWS THE TRANSACTION DATA IN THE WINDOW AND CONFIRMS THE TRANSACTION BY PROVIDING VALID BIOMETRIC DATA OR DENIES THE TRANSACTION BY CANCELING THE WINDOW/TRANSACTION
A
B

FIG. 2A

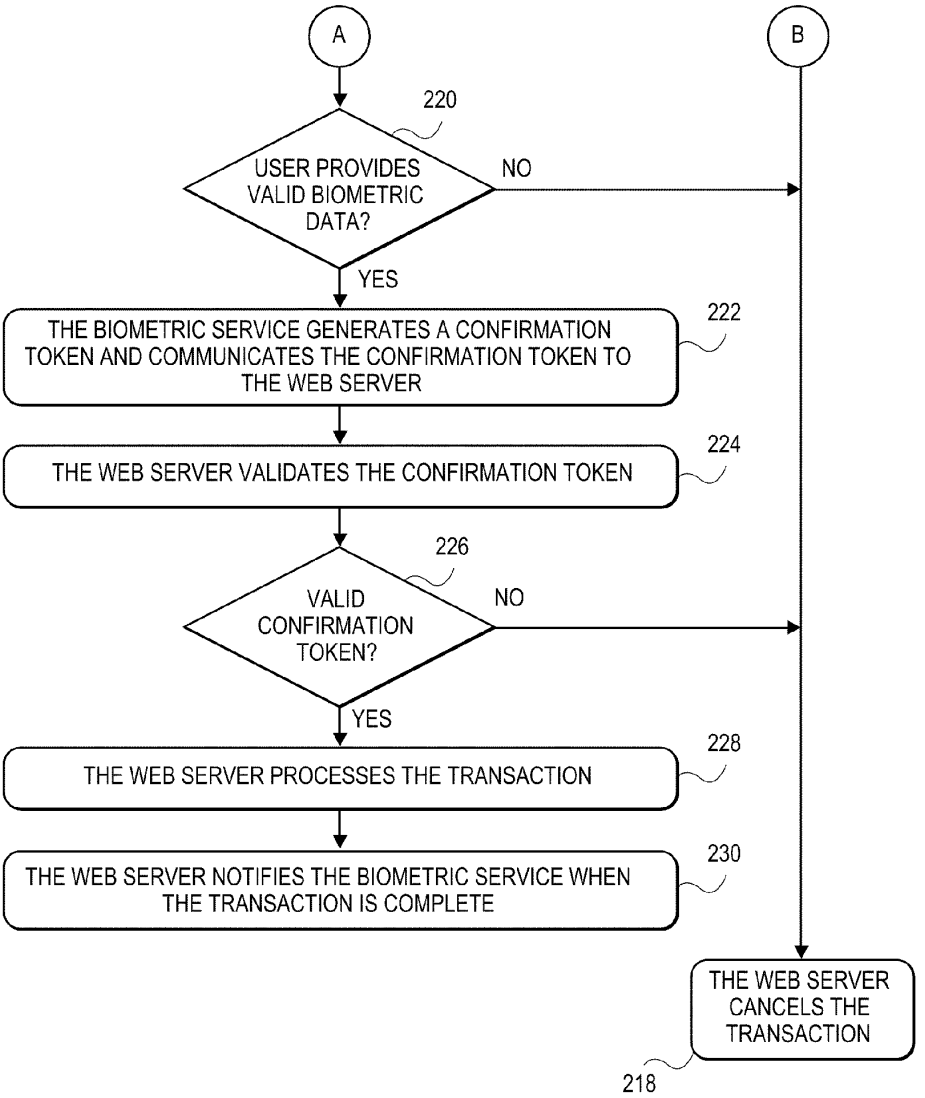

A
B
220
USER PROVIDES VALID BIOMETRIC DATA?
NO
YES
222
THE BIOMETRIC SERVICE GENERATES A CONFIRMATION TOKEN AND COMMUNICATES THE CONFIRMATION TOKEN TO THE WEB SERVER
224
THE WEB SERVER VALIDATES THE CONFIRMATION TOKEN
226
VALID CONFIRMATION TOKEN?
NO
YES
228
THE WEB SERVER PROCESSES THE TRANSACTION
230
THE WEB SERVER NOTIFIES THE BIOMETRIC SERVICE WHEN THE TRANSACTION IS COMPLETE
THE WEB SERVER CANCELS THE TRANSACTION
218

FIG. 2B

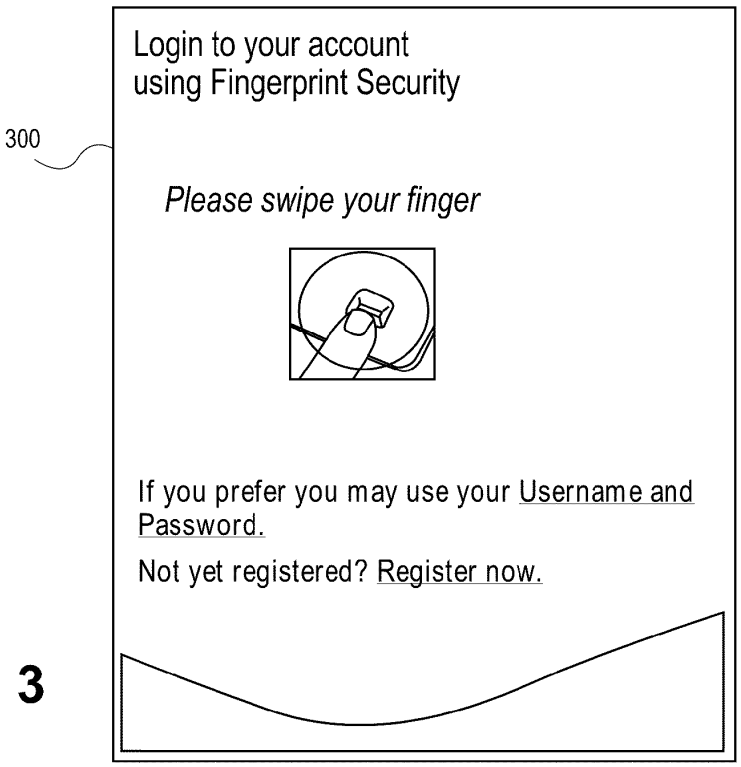

Login to your account
using Fingerprint Security
300
Please swipe your finger
If you prefer you may use your Username and Password.
Not yet registered? Register now.

FIG. 3

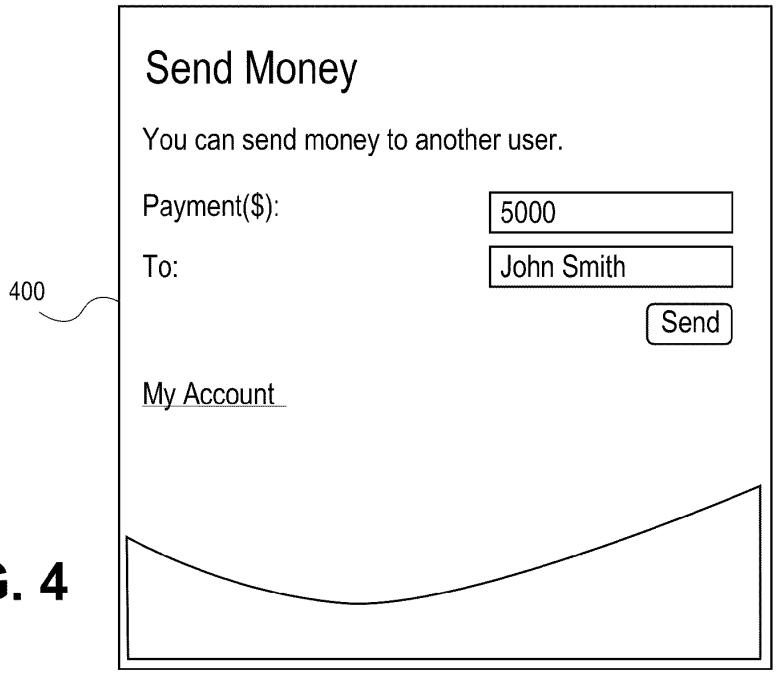

Send Money
You can send money to another user.
Payment($):
5000
To:
John Smith
400
Send
My Account

FIG. 4

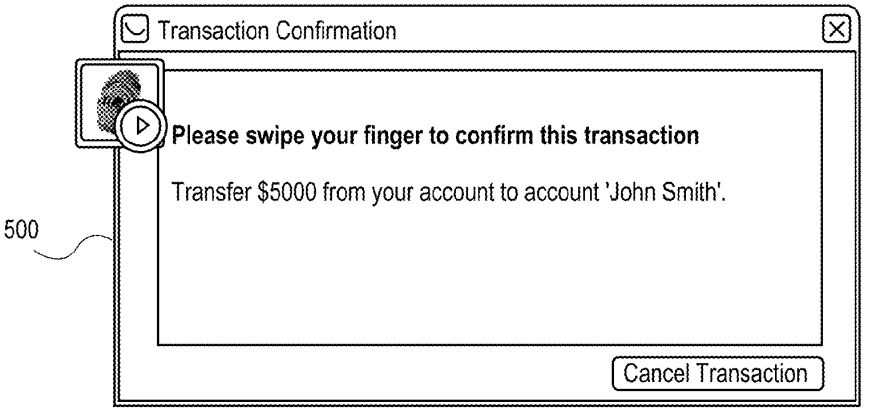

Transaction Confirmation
Please swipe your finger to confirm this transaction
Transfer $5000 from your account to account 'John Smith'.
500
Cancel Transaction

FIG. 5

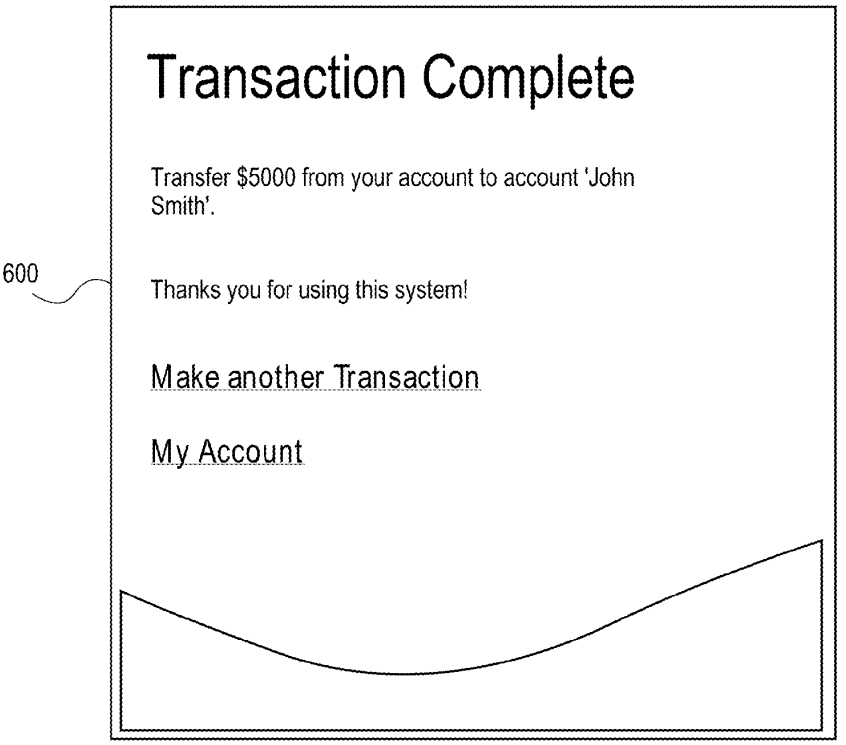

Transaction Complete
Transfer $5000 from your account to account 'John Smith'.
600
Thanks you for using this system!
Make another Transaction
My Account

FIG. 6

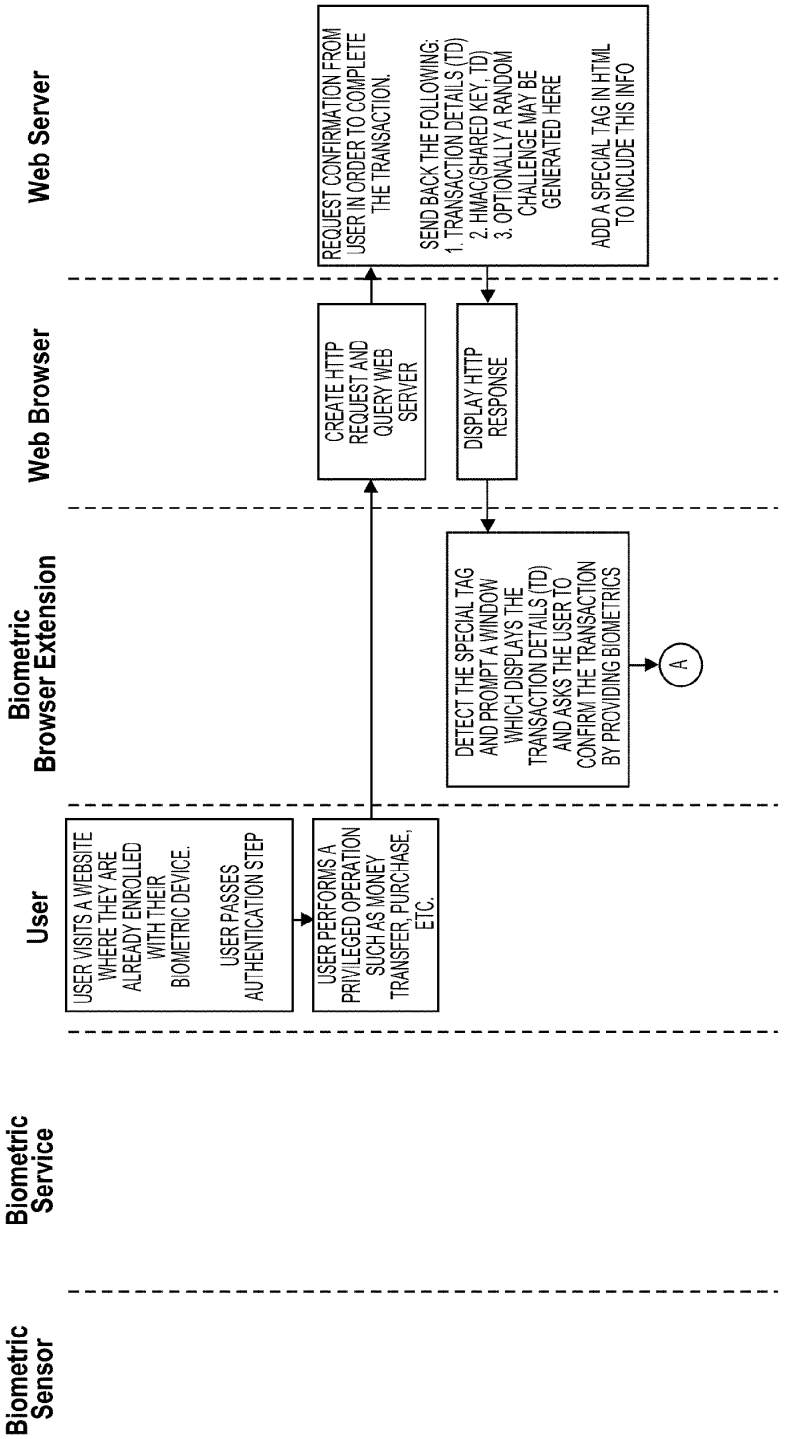

Biometric Sensor
Biometric Service
User
Biometric Browser Extension
Web Browser
Web Server
USER VISITS A WEBSITE WHERE THEY ARE ALREADY ENROLLED WITH THEIR BIOMETRIC DEVICE.
USER PASSES AUTHENTICATION STEP
USER PERFORMS A PRIVILEGED OPERATION SUCH AS MONEY TRANSFER, PURCHASE, ETC.
CREATE HTTP REQUEST AND QUERY WEB SERVER
REQUEST CONFIRMATION FROM USER IN ORDER TO COMPLETE THE TRANSACTION.
SEND BACK THE FOLLOWING:
1. TRANSACTION DETAILS (TD)
2. HMAC(SHARED KEY, TD)
3. OPTIONALLY A RANDOM CHALLENGE MAY BE GENERATED HERE
ADD A SPECIAL TAG IN HTML TO INCLUDE THIS INFO
DISPLAY HTTP RESPONSE
DETECT THE SPECIAL TAG AND PROMPT A WINDOW WHICH DISPLAYS THE TRANSACTION DETAILS (TD) AND ASKS THE USER TO CONFIRM THE TRANSACTION BY PROVIDING BIOMETRICS
A

FIG. 7A

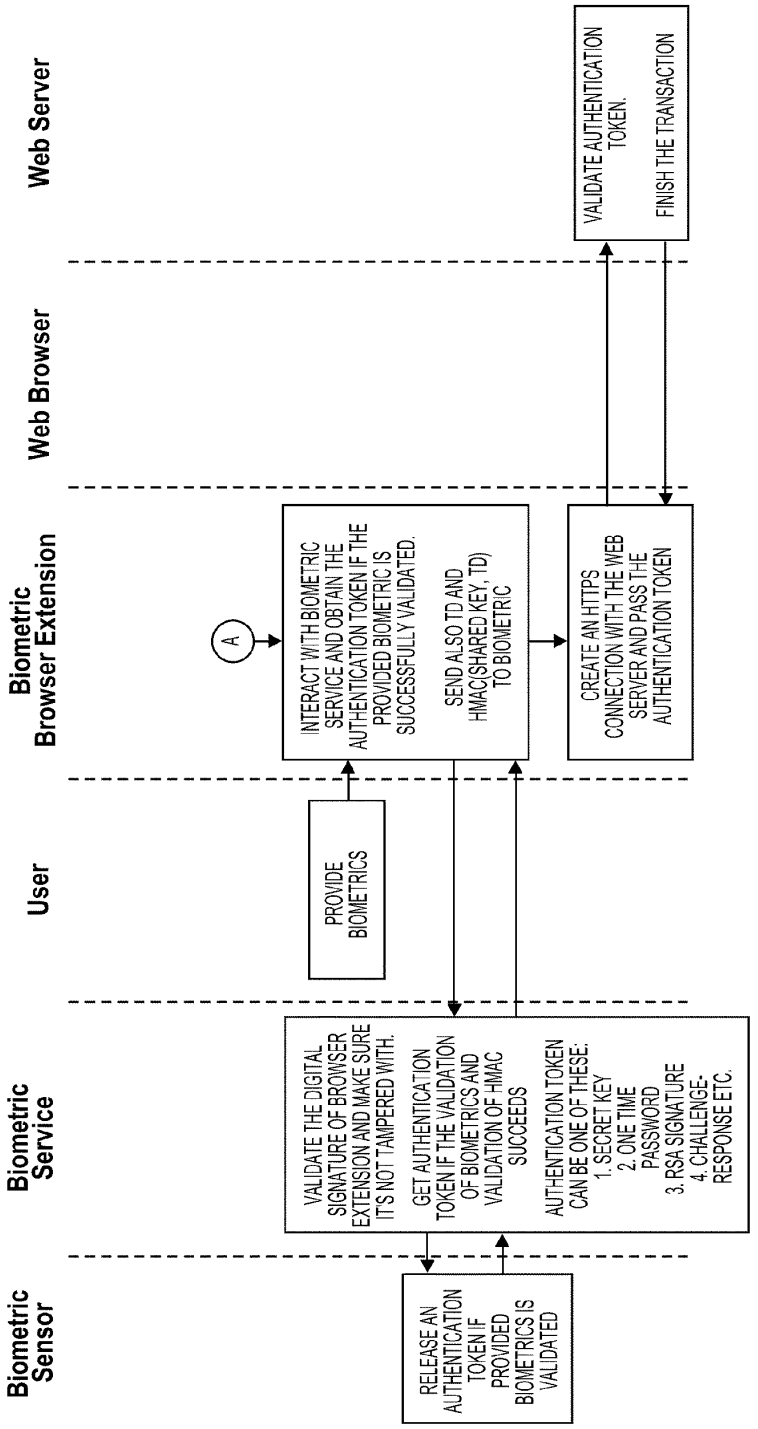

Biometric Sensor
Biometric Service
User
Biometric Browser Extension
Web Browser
Web Server
RELEASE AN AUTHENTICATION TOKEN IF PROVIDED BIOMETRICS IS VALIDATED
VALIDATE THE DIGITAL SIGNATURE OF BROWSER EXTENSION AND MAKE SURE ITS NOT TAMPERED WITH.
GET AUTHENTICATION TOKEN IF THE VALIDATION OF BIOMETRICS AND VALIDATION OF HMAC SUCCEEDS
AUTHENTICATION TOKEN CAN BE ONE OF THESE:
1. SECRET KEY
2. ONE TIME PASSWORD
3. RSA SIGNATURE
4. CHALLENGE-RESPONSE ETC.
PROVIDE BIOMETRICS
A
INTERACT WITH BIOMETRIC SERVICE AND OBTAIN THE AUTHENTICATION TOKEN IF THE PROVIDED BIOMETRIC IS SUCCESSFULLY VALIDATED.
SEND ALSO TD AND HMAC(SHARED KEY, TD) TO BIOMETRIC
CREATE AN HTTPS CONNECTION WITH THE WEB SERVER AND PASS THE AUTHENTICATION TOKEN
VALIDATE AUTHENTICATION TOKEN.
FINISH THE TRANSACTION

FIG. 7B

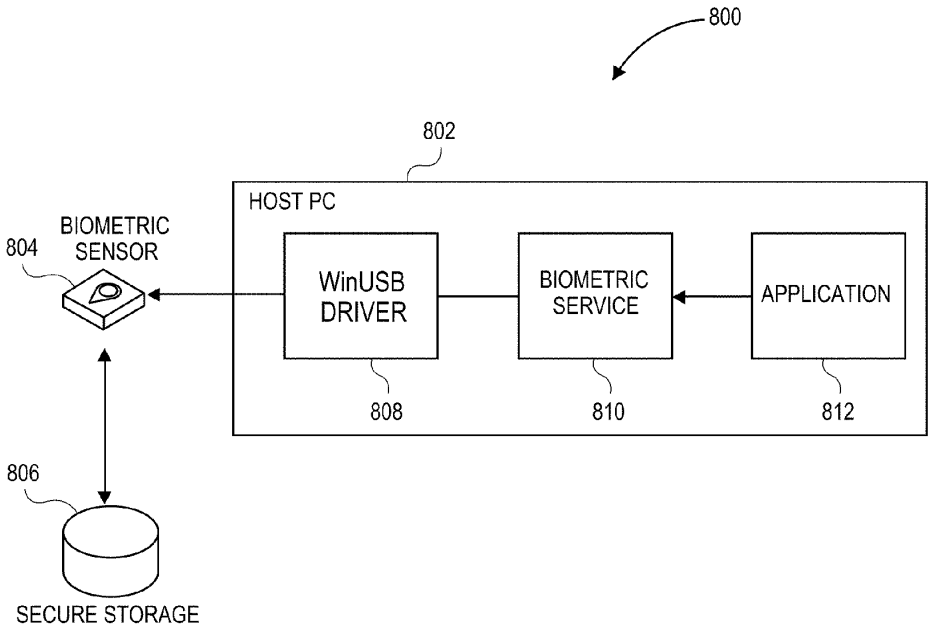

800
802
HOST PC
BIOMETRIC SENSOR
804
WinUSB DRIVER
BIOMETRIC SERVICE
APPLICATION
808
810
812
806
SECURE STORAGE

FIG. 8

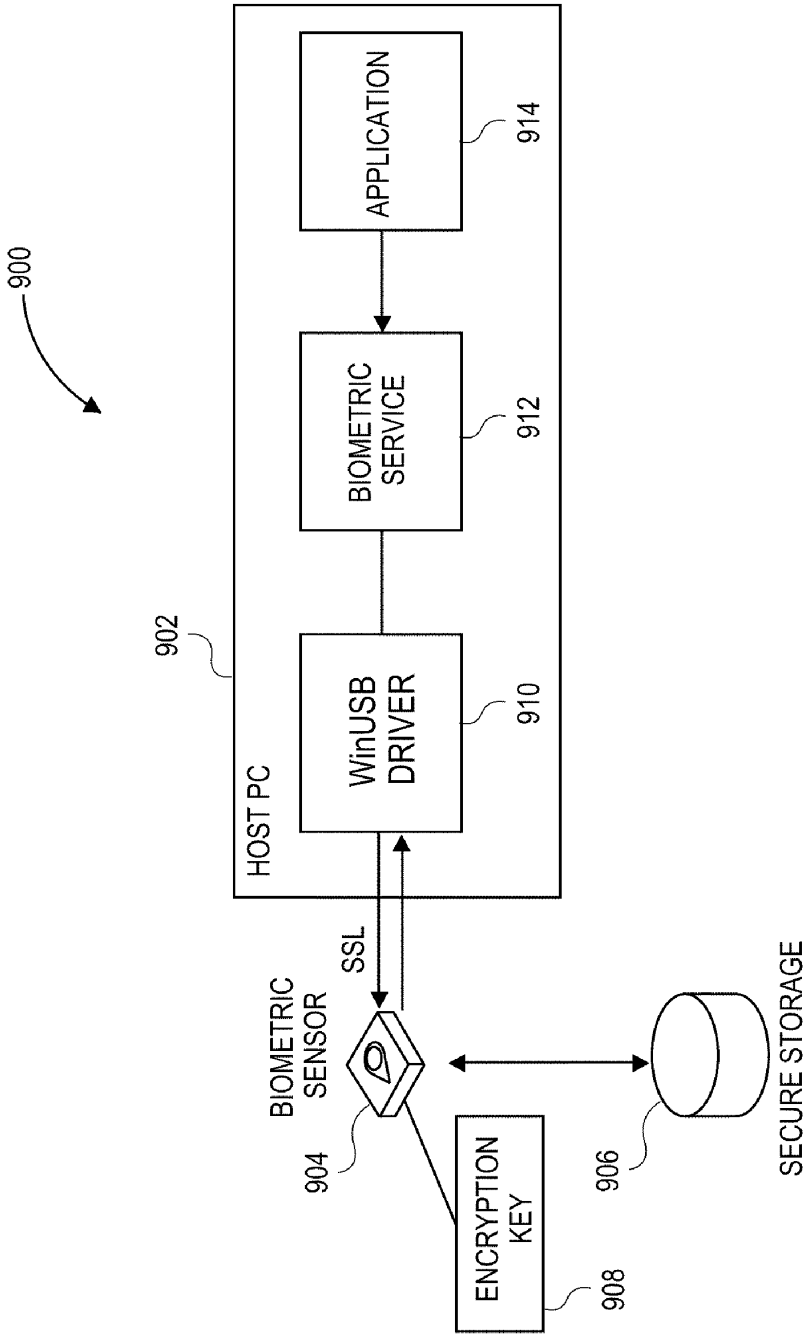

900
902
HOST PC
APPLICATION
914
BIOMETRIC SERVICE
912
WinUSB DRIVER
910
SSL
BIOMETRIC SENSOR
904
ENCRYPTION KEY
908
906
SECURE STORAGE

FIG. 9

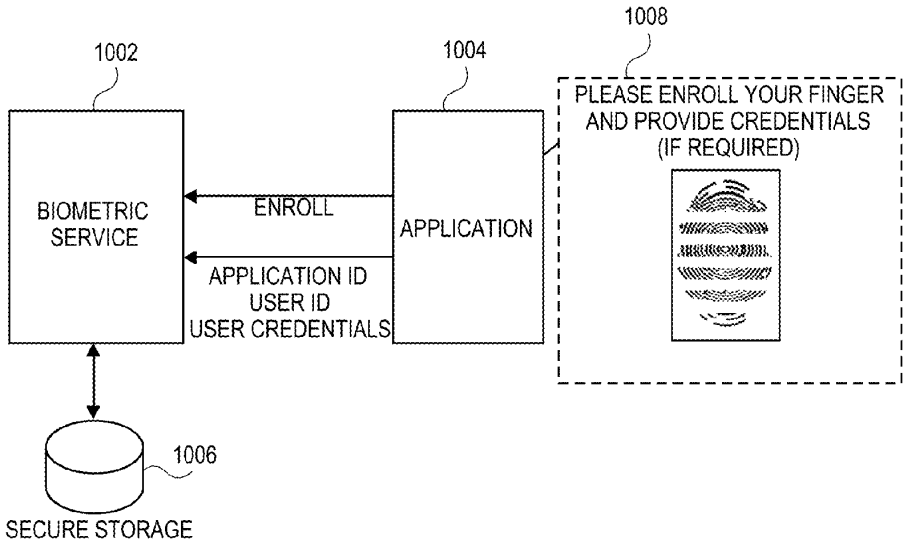

1002
1004
1008
BIOMETRIC SERVICE
ENROLL
APPLICATION ID
USER ID
USER CREDENTIALS
APPLICATION
PLEASE ENROLL YOUR FINGER AND PROVIDE CREDENTIALS (IF REQUIRED)
1006
SECURE STORAGE

FIG. 10

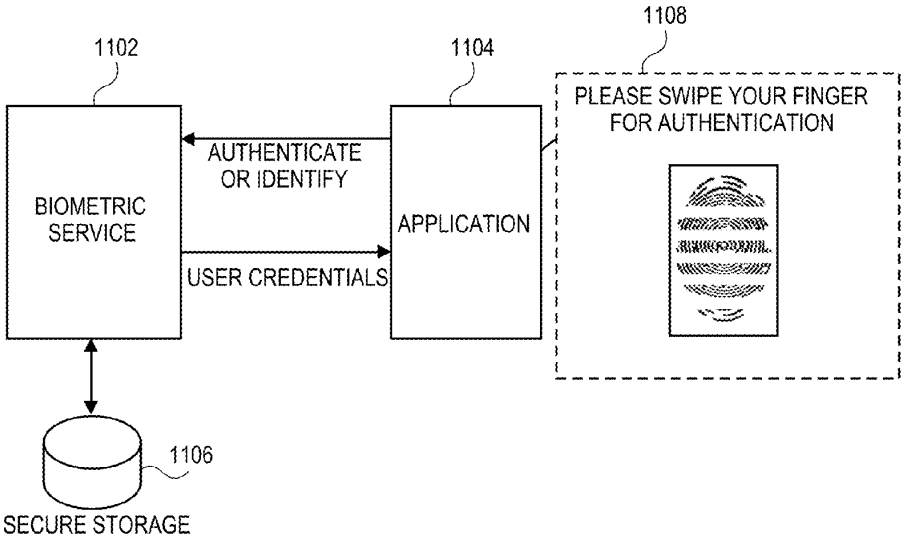

1102
1104
1108
BIOMETRIC SERVICE
AUTHENTICATE OR IDENTIFY
USER CREDENTIALS
APPLICATION
PLEASE SWIPE YOUR FINGER FOR AUTHENTICATION
1106
SECURE STORAGE

FIG. 11

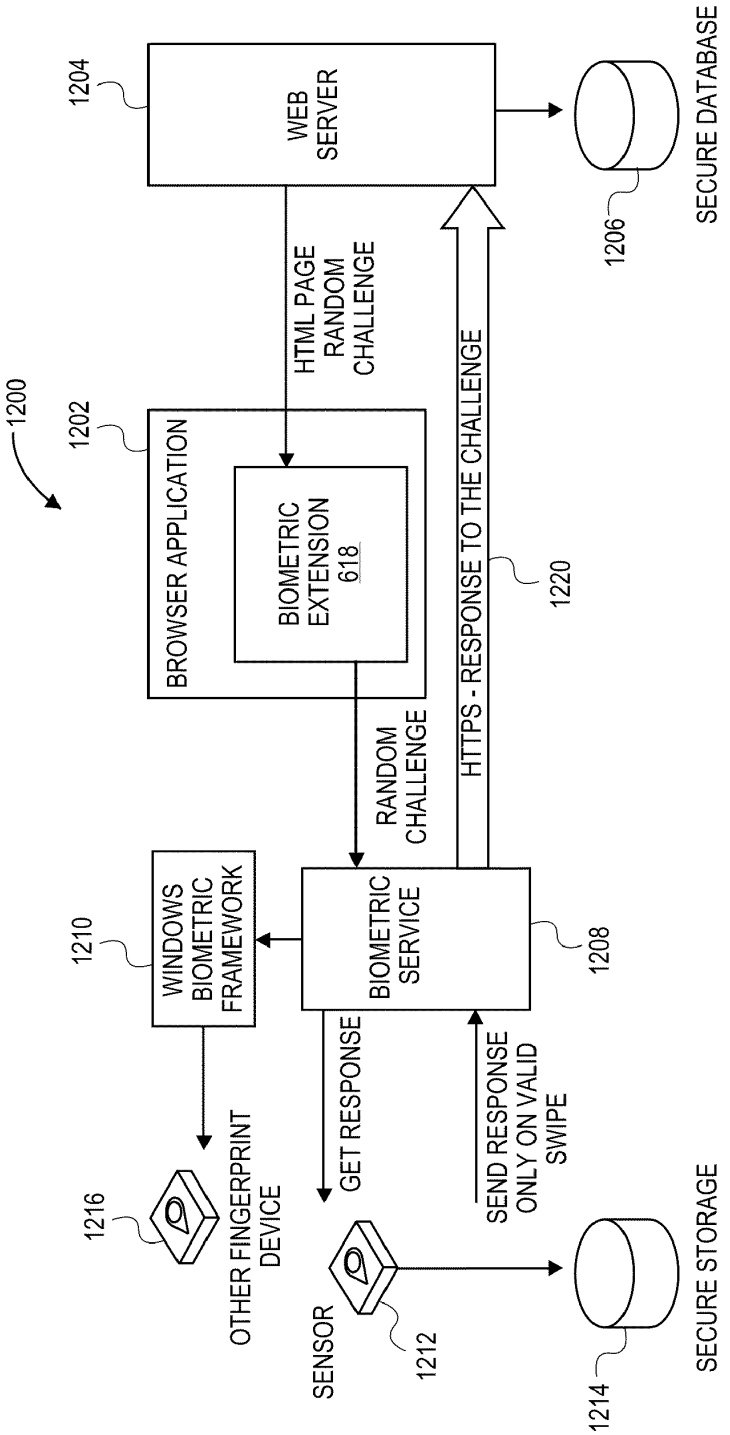

1200
1202
BROWSER APPLICATION
BIOMETRIC EXTENSION 618
HTML PAGE RANDOM CHALLENGE
1204
WEB SERVER
1206
SECURE DATABASE
HTTPS - RESPONSE TO THE CHALLENGE
1220
RANDOM CHALLENGE
1208
BIOMETRIC SERVICE
1210
WINDOWS BIOMETRIC FRAMEWORK
GET RESPONSE
SEND RESPONSE ONLY ON VALID SWIPE
1216
OTHER FINGERPRINT DEVICE
SENSOR
1212
1214
SECURE STORAGE

FIG. 12

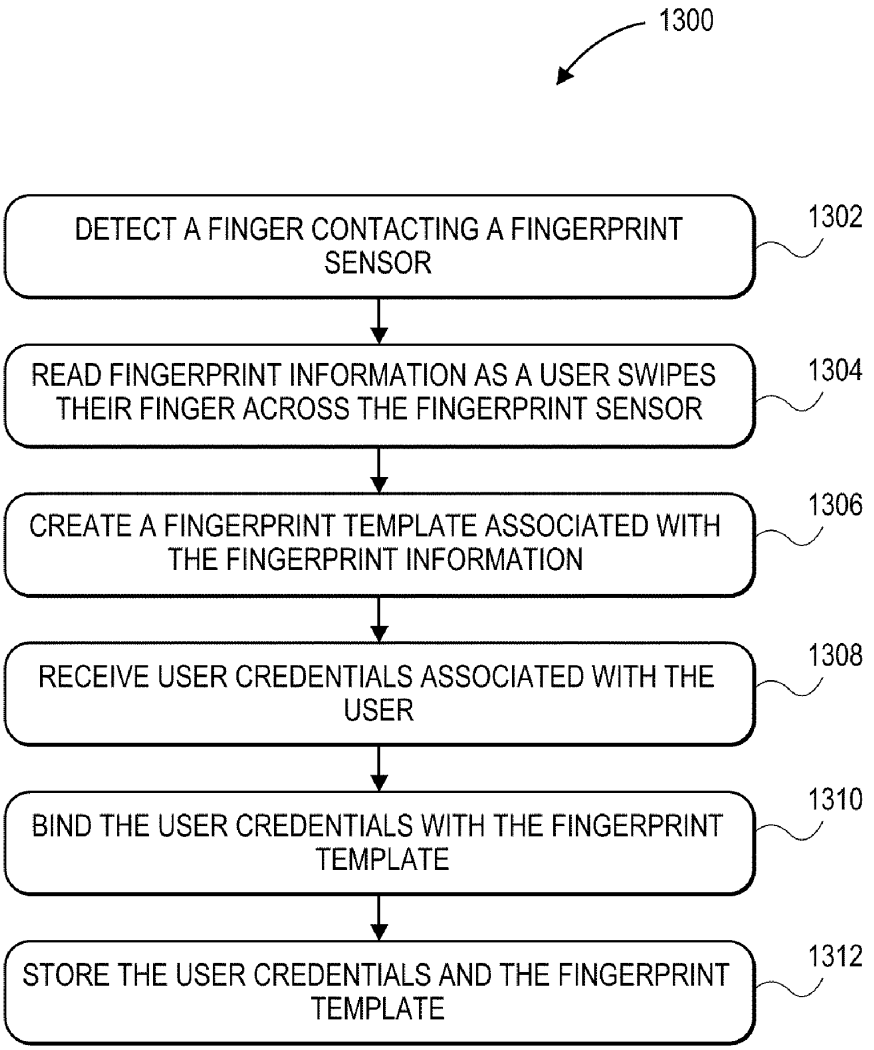

1300
DETECT A FINGER CONTACTING A FINGERPRINT SENSOR
1302
READ FINGERPRINT INFORMATION AS A USER SWIPES THEIR FINGER ACROSS THE FINGERPRINT SENSOR
1304
CREATE A FINGERPRINT TEMPLATE ASSOCIATED WITH THE FINGERPRINT INFORMATION
1306
RECEIVE USER CREDENTIALS ASSOCIATED WITH THE USER
1308
BIND THE USER CREDENTIALS WITH THE FINGERPRINT TEMPLATE
1310
STORE THE USER CREDENTIALS AND THE FINGERPRINT TEMPLATE
1312

FIG. 13

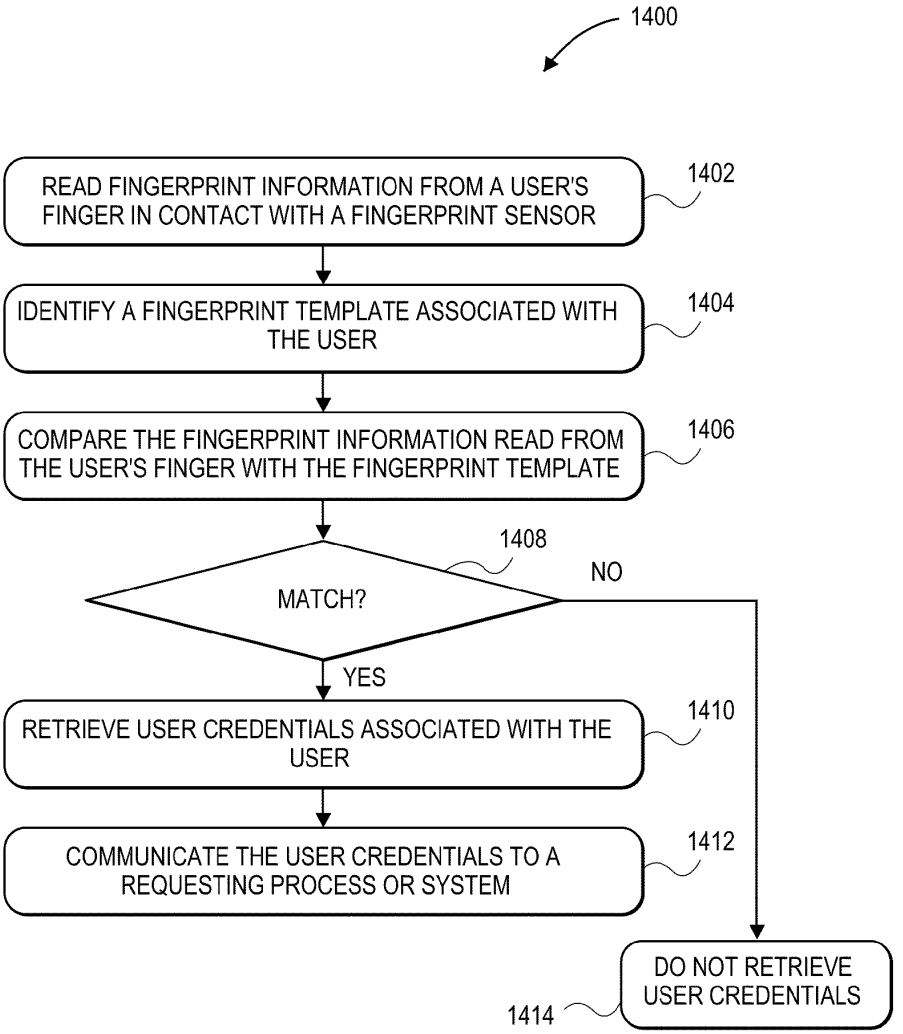

1400
READ FINGERPRINT INFORMATION FROM A USER'S FINGER IN CONTACT WITH A FINGERPRINT SENSOR
1402
IDENTIFY A FINGERPRINT TEMPLATE ASSOCIATED WITH THE USER
1404
COMPARE THE FINGERPRINT INFORMATION READ FROM THE USER'S FINGER WITH THE FINGERPRINT TEMPLATE
1406
1408
MATCH?
NO
YES
RETRIEVE USER CREDENTIALS ASSOCIATED WITH THE USER
1410
COMMUNICATE THE USER CREDENTIALS TO A REQUESTING PROCESS OR SYSTEM
1412
DO NOT RETRIEVE USER CREDENTIALS
1414

FIG. 14

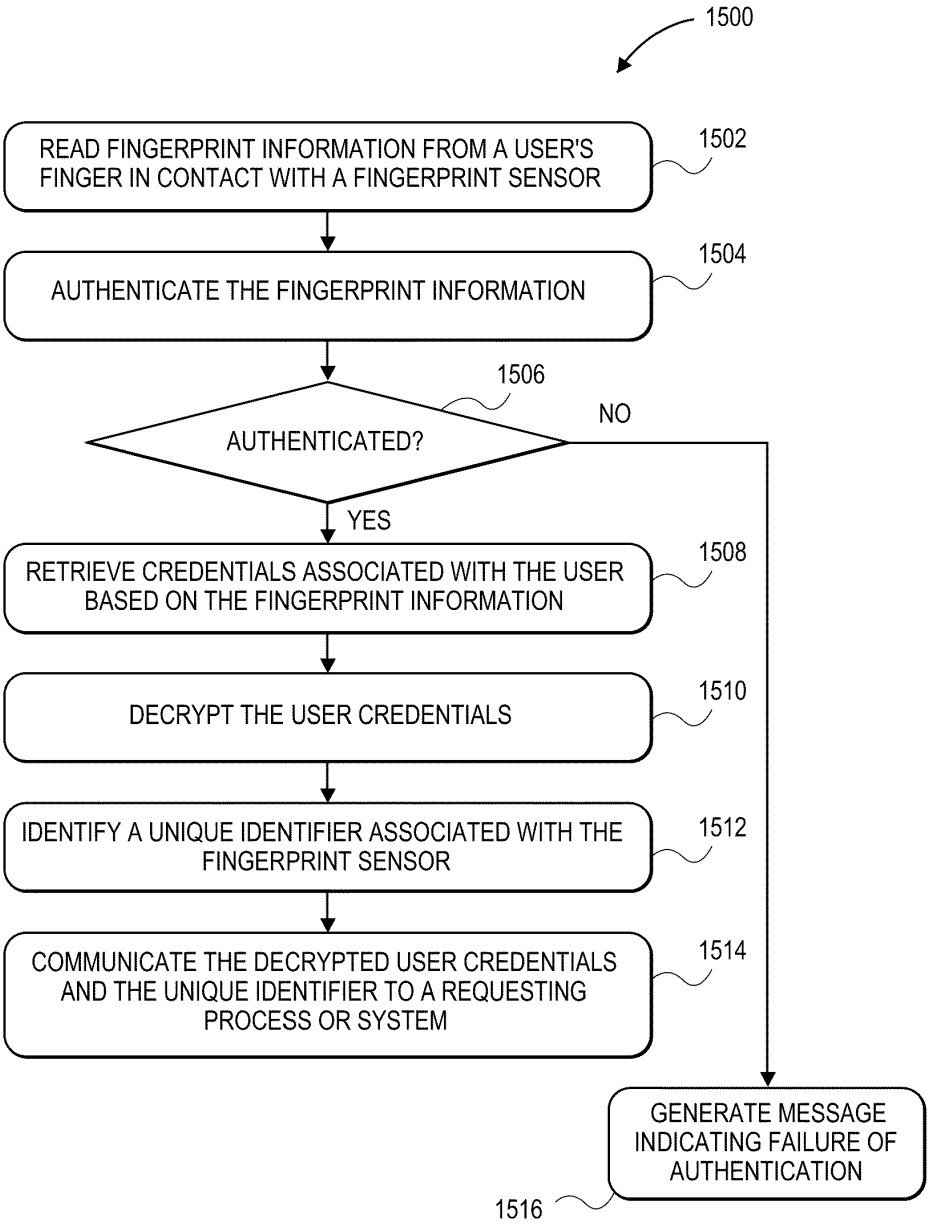

1500
READ FINGERPRINT INFORMATION FROM A USER'S FINGER IN CONTACT WITH A FINGERPRINT SENSOR
1502
AUTHENTICATE THE FINGERPRINT INFORMATION
1504
1506
AUTHENTICATED?
NO
YES
RETRIEVE CREDENTIALS ASSOCIATED WITH THE USER BASED ON THE FINGERPRINT INFORMATION
1508
DECRYPT THE USER CREDENTIALS
1510
IDENTIFY A UNIQUE IDENTIFIER ASSOCIATED WITH THE FINGERPRINT SENSOR
1512
COMMUNICATE THE DECRYPTED USER CREDENTIALS AND THE UNIQUE IDENTIFIER TO A REQUESTING PROCESS OR SYSTEM
1514
GENERATE MESSAGE INDICATING FAILURE OF AUTHENTICATION
1516

FIG. 15

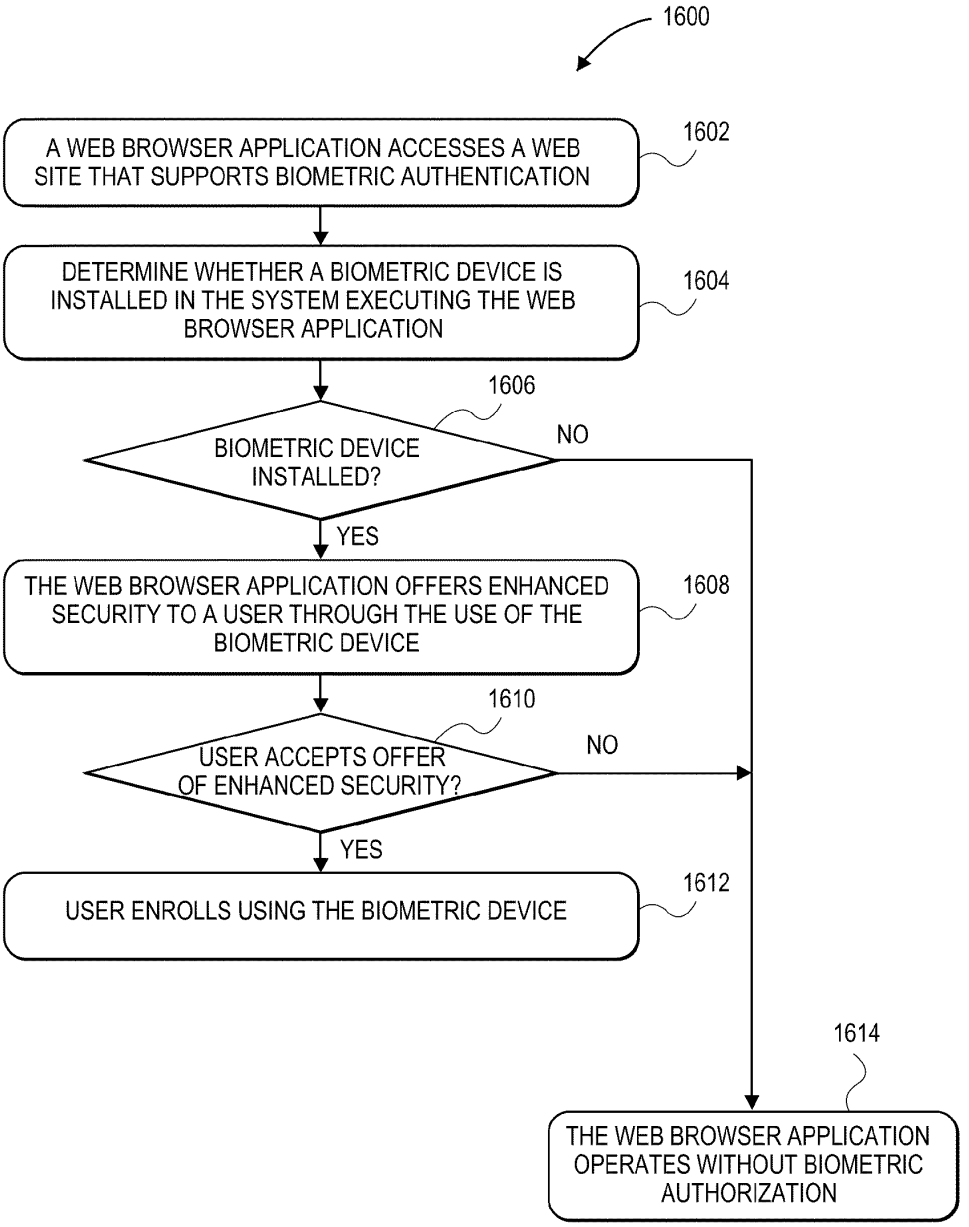

1600
A WEB BROWSER APPLICATION ACCESSES A WEB SITE THAT SUPPORTS BIOMETRIC AUTHENTICATION
1602
DETERMINE WHETHER A BIOMETRIC DEVICE IS INSTALLED IN THE SYSTEM EXECUTING THE WEB BROWSER APPLICATION
1604
1606
BIOMETRIC DEVICE INSTALLED?
NO
YES
THE WEB BROWSER APPLICATION OFFERS ENHANCED SECURITY TO A USER THROUGH THE USE OF THE BIOMETRIC DEVICE
1608
1610
USER ACCEPTS OFFER OF ENHANCED SECURITY?
NO
YES
USER ENROLLS USING THE BIOMETRIC DEVICE
1612
1614
THE WEB BROWSER APPLICATION OPERATES WITHOUT BIOMETRIC AUTHORIZATION

FIG. 16

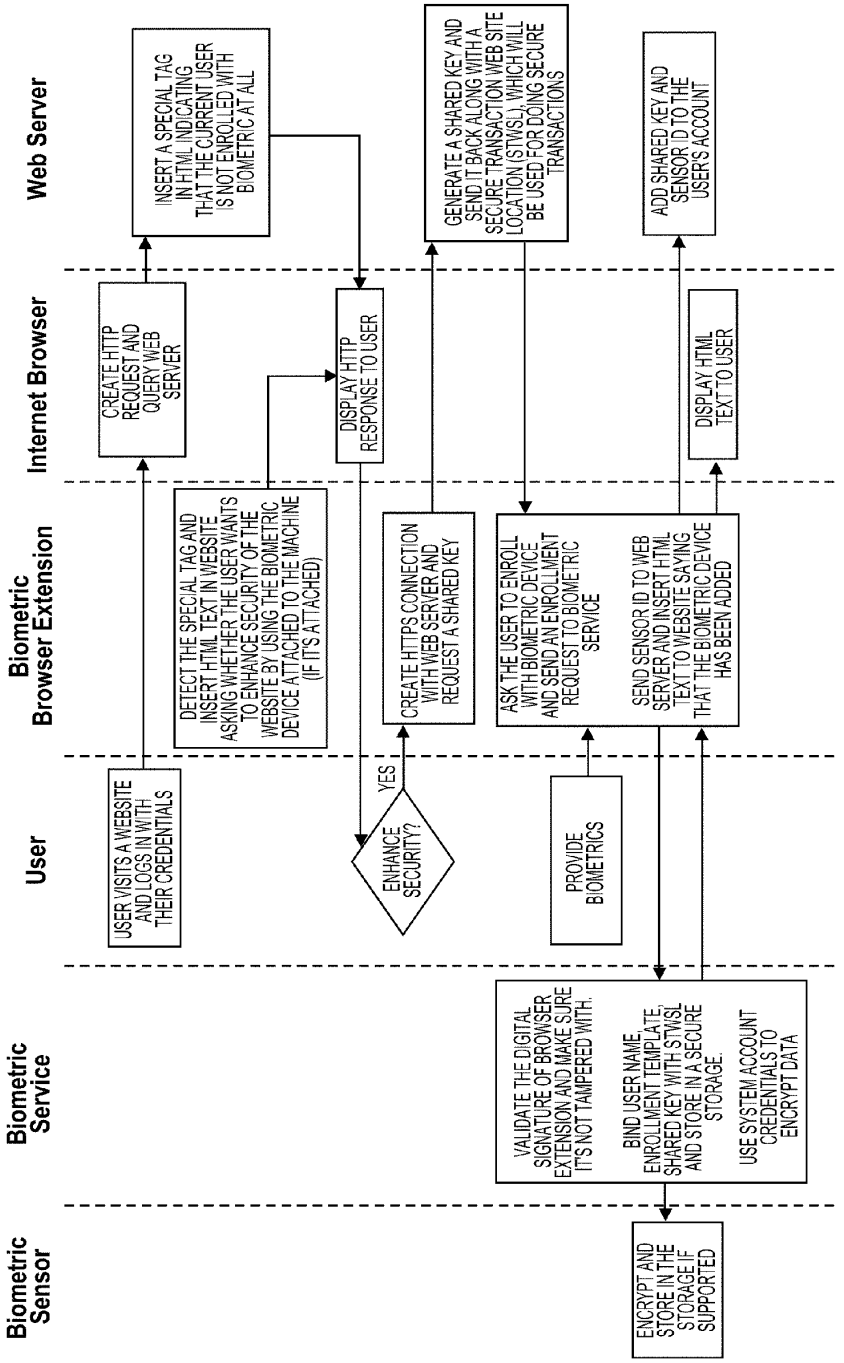

Web Server
Internet Browser
Biometric Browser Extension
User
Biometric Service
Biometric Sensor
INSERT A SPECIAL TAG IN HTML INDICATING THAT THE CURRENT USER IS NOT ENROLLED WITH BIOMETRIC AT ALL
GENERATE A SHARED KEY AND SEND IT BACK ALONG WITH A SECURE TRANSACTION WEB SITE LOCATION (STWSL), WHICH WILL BE USED FOR DOING SECURE TRANSACTIONS
ADD SHARED KEY AND SENSOR ID TO THE USER'S ACCOUNT
CREATE HTTP REQUEST AND QUERY WEB SERVER
DISPLAY HTTP RESPONSE TO USER
DISPLAY HTML TEXT TO USER
DETECT THE SPECIAL TAG AND INSERT HTML TEXT IN WEBSITE ASKING WHETHER THE USER WANTS TO ENHANCE SECURITY OF THE WEBSITE BY USING THE BIOMETRIC DEVICE ATTACHED TO THE MACHINE (IF IT'S ATTACHED)
CREATE HTTPS CONNECTION WITH WEB SERVER AND REQUEST A SHARED KEY
ASK THE USER TO ENROLL WITH BIOMETRIC DEVICE AND SEND AN ENROLLMENT REQUEST TO BIOMETRIC SERVICE
SEND SENSOR ID TO WEB SERVER AND INSERT HTML TEXT TO WEBSITE SAYING THAT THE BIOMETRIC DEVICE HAS BEEN ADDED
USER VISITS A WEBSITE AND LOGS IN WITH THEIR CREDENTIALS
YES
ENHANCE SECURITY?
PROVIDE BIOMETRICS
VALIDATE THE DIGITAL SIGNATURE OF BROWSER EXTENSION AND MAKE SURE IT'S NOT TAMPERED WITH.
BIND USER NAME, ENROLLMENT TEMPLATE, SHARED KEY WITH STWSL AND STORE IN A SECURE STORAGE.
USE SYSTEM ACCOUNT CREDENTIALS TO ENCRYPT DATA
ENCRYPT AND STORE IN THE STORAGE IF SUPPORTED

FIG. 17

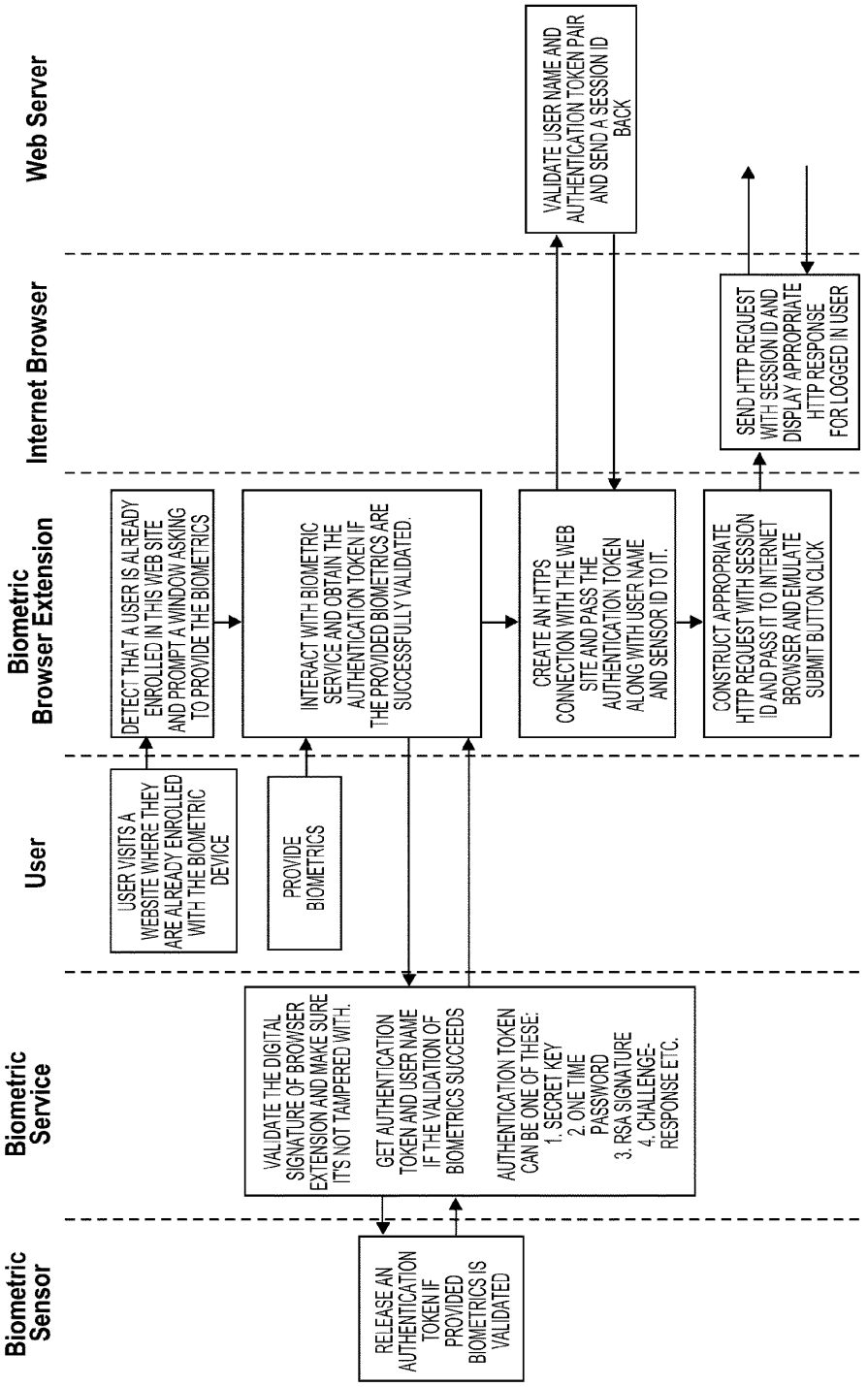

Biometric Sensor
Biometric Service
User
Biometric Browser Extension
Internet Browser
Web Server
RELEASE AN AUTHENTICATION TOKEN IF PROVIDED BIOMETRICS IS VALIDATED
VALIDATE THE DIGITAL SIGNATURE OF BROWSER EXTENSION AND MAKE SURE ITS NOT TAMPERED WITH.
GET AUTHENTICATION TOKEN AND USER NAME IF THE VALIDATION OF BIOMETRICS SUCCEEDS
AUTHENTICATION TOKEN CAN BE ONE OF THESE:
1. SECRET KEY
2. ONE TIME PASSWORD
3. RSA SIGNATURE
4. CHALLENGE-RESPONSE ETC.
USER VISITS A WEBSITE WHERE THEY ARE ALREADY ENROLLED WITH THE BIOMETRIC DEVICE
PROVIDE BIOMETRICS
DETECT THAT A USER IS ALREADY ENROLLED IN THIS WEB SITE AND PROMPT A WINDOW ASKING TO PROVIDE THE BIOMETRICS
INTERACT WITH BIOMETRIC SERVICE AND OBTAIN THE AUTHENTICATION TOKEN IF THE PROVIDED BIOMETRICS ARE SUCCESSFULLY VALIDATED.
CREATE AN HTTPS CONNECTION WITH THE WEB SITE AND PASS THE AUTHENTICATION TOKEN ALONG WITH USER NAME AND SENSOR ID TO IT.
VALIDATE USER NAME AND AUTHENTICATION TOKEN PAIR AND SEND A SESSION ID BACK
CONSTRUCT APPROPRIATE HTTP REQUEST WITH SESSION ID AND PASS IT TO INTERNET BROWSER AND EMULATE SUBMIT BUTTON CLICK
SEND HTTP REQUEST WITH SESSION ID AND DISPLAY APPROPRIATE HTTP RESPONSE FOR LOGGED IN USER

FIG. 18

SECURE TRANSACTION SYSTEMS AND METHODS USING USER AUTHENTICATING BIOMETRIC INFORMATION

RELATED APPLICATIONS

[0001] This application claims the benefit of U.S. Provisional Application No. 61/249,218, filed Oct. 6, 2009, the disclosure of which is incorporated by reference herein. This application also claims the benefit of U.S. Provisional Application No. 61/292,820, filed Jan. 6, 2010. This application also references the following U.S. Non-Provisional Applications: U.S. Non-Provisional application Ser. No. 12/731,027, filed Mar. 24, 2010, U.S. Non-Provisional application Ser. No. 12/731,037, filed Mar. 24, 2010, U.S. Non-Provisional application Ser. No. 12/731,050, filed Mar. 24, 2010, U.S. Non-Provisional application Ser. No. 12/751,952, filed Mar. 31, 2010, U.S. Non-Provisional application Ser. No. 12/751,964, filed Mar. 31, 2010, U.S. Non-Provisional application Ser. No. 12/751,983, filed Mar. 31, 2010, U.S. Non-Provisional application Ser. No. 12/751,954, filed Mar. 31, 2010, and U.S. Non-Provisional application Ser. No. 12/751,969, filed Mar. 31, 2010. All of these co-pending applications are incorporated by reference herein.

BACKGROUND

[0002] Typical user authentication systems and procedures use passwords to authenticate the identity of the user. In many instances, Web sites are authenticated using SSL (Secure Sockets Layer) or other protocols. SSL is a protocol for securely transmitting information via the Internet. When using SSL, a Web site is authenticated via its certificate. The user seeking access to the Web site is then authenticated by username and password.

[0003] Although passwords are commonly used to authenticate users, passwords are subject to various attacks, such as phishing attacks, social engineering attacks, dictionary attacks and the like. Typically, longer passwords with combinations of letters and numbers provide a higher level of security. However, these longer passwords are more difficult for users to remember. Additionally, passwords provide a single factor of authentication by requiring the user to provide something they know. This factor does not provide any physical authentication of the user's identity. Thus, any person can access the user's Web-based accounts and information if they gain knowledge of the user's password and username. Additionally, anyone with knowledge of a user's password can initiate transactions (e.g., purchase transactions and fund transfers) without the user's permission.

[0004] Another potential threat that occurs when using passwords is commonly referred to as "Man in the Browser" attacks. These types of attacks involve malicious software applications (malware) running in the internet browser while the user is logging on to a web site or performing a financial transaction.

[0005] One of the implementations of this attack is to get access to user's password when the user provides their password to the internet browser. After this point malware can conduct any type of malicious action with the user's account.

[0006] Another example of a "Man in the Browser" attack is to modify the transaction information on the fly and dupe the user by encouraging them to confirm a transaction which they didn't intend to confirm. The malware residing in the internet browser has full access to all graphical user interface parts of the browser (window, text, etc.) and may change them whenever necessary. Therefore, it's important to not trust the browser user interface when conducting important financial operations or when logging in to a web account.

[0007] Therefore, it is desirable to provide a user authentication method and system that offers a more secure authentication of the user, and more secure transactions, than commonly used password-based systems and methods.

BRIEF DESCRIPTION OF THE DRAWINGS

[0008] FIG. **1** depicts an example system capable of implementing secure transactions as discussed herein.

[0009] FIGS. **2**A and **2**B represent a flow diagram depicting an embodiment of a procedure for implementing a secure transaction.

[0010] FIGS. **3**-**6** depict example user interface displays for implementing secure transactions.

[0011] FIGS. **7**A and **7**B depict another example of a procedure for implementing a secure transaction.

[0012] FIG. **8** depicts an example system capable of performing biometric user authentication.

[0013] FIG. **9** depicts another example system capable of performing biometric user authentication.

[0014] FIG. **10** depicts an example user enrollment process.

[0015] FIG. **11** depicts an example user authentication process.

[0016] FIG. **12** depicts another example system capable of performing biometric user authentication.

[0017] FIG. **13** is a flow diagram depicting an embodiment of a procedure for enrolling a user of a biometric authentication system.

[0018] FIG. **14** is a flow diagram depicting an embodiment of a procedure for authenticating a user of a biometric authentication system.

[0019] FIG. **15** is a flow diagram depicting another embodiment of a procedure for authenticating a user of a biometric authentication system.

[0020] FIG. **16** is a flow diagram depicting an embodiment of a procedure for authenticating a user of a Web browser application that supports biometric authentication.

[0021] FIG. **17** depicts another embodiment of a procedure for enrolling a user of a biometric authentication system.

[0022] FIG. **18** depicts another embodiment of a procedure for identifying and authenticating a user of a biometric authentication system.

[0023] Throughout the description, similar reference numbers may be used to identify similar elements.

DETAILED DESCRIPTION

[0024] The systems and methods described herein relate to biometric authentication of users. "Biometrics", "biometric information" and "biometric data" refers to measurable biological characteristics of a user, such as fingerprint characteristics, facial characteristics, eye characteristics, voice characteristics (also referred to as a "voiceprint") and the like. As discussed herein, biometric information provides an additional level of security when used in systems and procedures related to authentication of a user and the implementation of secure transactions.

[0025] Particular examples discussed herein use fingerprint biometric information to authenticate one or more users. In other embodiments, any type of biometric information may be used instead of fingerprint information. Additionally, a

particular embodiment may utilize multiple types of biometric information (e.g., fingerprints and voiceprints) to authenticate a user. Certain described embodiments refer to "swipe" style fingerprint sensors. However, alternate embodiments may include any type of fingerprint sensor, such as a "placement" sensor. In particular embodiments, the biometric sensor is physically attached (or manufactured into) a client device, such as a computer, cellular phone, and so forth. In other embodiments, the biometric sensor is a portable device that is temporarily coupled to the client device (e.g., a pluggable USB device) for enrollment, authentication and/or secure transaction procedures.

[0026] As used herein, a "web application", a "web-based application", and a "web-enabled application" refers to a software application or software routine that is capable of communicating with one or more web servers or similar devices via the Internet or other data communication network. Additionally, a "plug-in", "browser plug-in" or a "browser extension" refers to an application or extension that provides a variety of different features and functions. Particular examples of "plug-ins" and "browser plug-ins" discussed herein provide features and functions related to user authentication while, for example, accessing web sites, implementing secure transactions, and the like. In particular embodiments, the browser plug-in is installed as part of the manufacturing process of devices equipped with associated biometric devices. In other embodiments, the browser plug-in is downloaded (e.g., via the Internet) at any time after the device is manufactured. In specific implementations, the browser plug-in is operable with any biometric device that supports the Windows Biometric Framework or other supported architectures or systems.

[0027] As discussed above, typical passwords do not provide any physical authentication of the user's identity. Thus, any person can access a user's Web-based accounts and related information if they gain knowledge of the user's password and username. Additionally, anyone with the user's password and username can initiate a transaction (such as a financial transaction) without the user's permission. Using biometric information in the user authentication and/or transaction process provides an increased level of security by authenticating physical characteristics of the user. Thus, an imposter with the correct password but lacking the required physical characteristics will not be authenticated by the system and not permitted to initiate a transaction needing user permission.

[0028] The systems and methods described herein perform biometric user authentication in several steps. A specific discussion of these user authentication steps is provided below.

[0029] FIG. **1** depicts an example system **100** capable of implementing secure transactions as discussed herein. A web browser application **102** executing on a user's computing device communicates with various web servers via the Internet. Web browser application **102** includes a browser extension **104** (or browser plug-in) that communicates with a biometric service **106**. In a particular embodiment, biometric service **106** is a secure application executing in a background mode on the user's computing device. Biometric service **106** provides a communication interface to a biometric sensor **108**, such as a fingerprint sensor. Embodiments of biometric sensor **108** may include a unique encryption key **110** and may store various information, such as user names, encrypted secret keys, and the like in a secure storage device **112**.

[0030] Browser extension **104** is capable of communicating transaction details, random challenges, signature information, and other data to biometric service **106**. Biometric service **106** verifies the digital signature of an agent application **114** prior to communicating with the agent application. Biometric service **106** may communicate transaction details and related information to agent application **114**. During a secure transaction, biometric service **106** also verifies the text presented in a transaction window **116** to the user until the user confirms the transaction by interacting with biometric sensor **108** (e.g., by presenting the user's fingerprint to a fingerprint sensor). Agent application **114** is responsible for launching transaction window **116** and displaying transaction information in the transaction window. Biometric service **106** communicates with one or more web servers as part of the user authentication procedure and during implementation of the secure transaction. Additional details regarding the enrollment and biometric authentication of a user are discussed below.

[0031] FIGS. **2**A and **2**B represent a flow diagram depicting an embodiment of a procedure **200** for implementing a secure transaction. A user submits a transaction to a web server via a web browser application (block **202**). This transaction may include a purchase transaction, a funds transfer transaction, or any other transaction in which the user desires a particular level of security. The web server returns the transaction signed with a key that is shared between the client device (the computing system executing the web browser application) and the web server (block **204**). The web server may also communicate additional data to the client device executing the web browser application (block **206**). This additional data may include transaction details, time and other information. For example, additional data may include a cryptographic nonce.

[0032] The web browser application receives the transaction data and any additional data, and communicates the received data to a biometric service (block **208**), such as biometric service **106** shown in FIG. **1**. The biometric service then generates a window and displays transaction data in the window (block **210**). This window is for the benefit of the user to view and confirm the transaction details. The biometric service then monitors the transaction data presented in the window to ensure that the presented data is not modified (block **212**), e.g., by a malicious application or a malicious user. If the biometric service detects that any of the data in the window is modified, the biometric service instructs the web server to cancel the transaction (block **218**). The biometric service may verify the integrity of the data in the window at regular (e.g., periodic) time intervals or at random time intervals.

[0033] If the data in the window is not modified, the user is then given the opportunity to review the transaction data presented in the window and either 1) confirm the transaction by providing valid biometric data; or 2) deny the transaction by canceling the window or canceling the transaction (block **216**). If the user does not provide valid biometric data (or the user closes the window/cancels the transaction), the biometric service instructs the web server to cancel the transaction (block **218**). If the user provides valid biometric data, the biometric service generates a confirmation token and communicates the confirmation token to the web server (block **222**). The web server then validates the confirmation token (block **224**). If the confirmation token is determined by the web server to be invalid, the web server cancels the transac-

tion (block **218**). However, if the confirmation is determined by the web server to be valid, the web server processes the transaction (block **228**) and notifies the biometric service when the transaction is complete (block **230**).

[0034] FIGS. **3-6** depict example user interface displays for implementing secure transactions. FIG. **3** shows an example user interface display **300** that gives the user an opportunity to login to the user's account. In this example, the user logs into the account by swiping their finger across a fingerprint sensor or activating another biometric device.

[0035] FIG. **4** shows an example user interface display **400** that allows the user to send funds to another user or to make a payment to a merchant or other person or entity. As shown in FIG. **4**, the user can enter the amount of the payment or funds transfer as well as the name of the recipient of the funds. In alternate embodiments, the user may also identify additional information such as a scheduled time for the transaction or a comment/note related to the transaction.

[0036] FIG. **5** shows an example user interface display **500** that allows a user to confirm a transaction by swiping their finger across a fingerprint sensor (or using another type of biometric device). The interface shown in FIG. **5** displays the transaction details, such as the amount of the funds transfer and the recipient of the funds. If the user chooses not to confirm the transaction, they can close the window shown in FIG. **5** or activate the "Cancel Transaction" button included in the display. To confirm the transaction, the user simply swipes their finger across the fingerprint sensor in their computing device. If the user swipes their fingerprint and the user's fingerprint information is verified, the web server processes the transaction. Upon completion of the transaction, the web server notifies the user that the transaction is complete by displaying a user interface window (such as example user interface **600** display shown in FIG. **6**) indicating completion of the transaction. User interface **600** shown in FIG. **6** also displays the details of the completed transaction to the user.

[0037] FIGS. **7**A and **7**B depict another example of a procedure for implementing a secure transaction. The example shown in FIGS. **7**A and **7**B includes various tasks, actions and functions performed by different systems, procedures or components, such as the biometric sensor, the biometric service, the user, the biometric browser extension, the internet browser application, and the web server. A user visits a web site where they previously enrolled their biometric information associated with a biometric device (e.g., a fingerprint sensor). If the user is authenticated, they can initiate a privileged operation, such as a secure transaction. This privileged operation may include transferring funds, purchasing a product or service, and the like.

[0038] The web browser application creates an HTTP request associated with the secure transaction and communicates the request to an appropriate web server. The web server requests information from the user to complete the requested secure transaction. The web server then returns various information, such as transaction details, a shared key, and a random challenge. This information returned by the web server is identified by a specific HTML tag inserted into the HTML code by the web server. Upon receiving this information from the web server, the web browser displays an appropriate response. The biometric browser extension detects the HTML tag inserted by the web server and requests the generation of a display window to display the transaction details and ask the user to confirm the transaction details by providing biometric authorization. The biometric browser extension interacts with the biometric service to obtain an authentication token if the user provides valid biometric information (e.g., a valid fingerprint is scanned by a fingerprint sensor).

[0039] The biometric service validates the digital signature of the biometric browser extension to be certain the biometric browser extension has not been modified or experienced any tampering. If the user provides valid biometric authorization and the biometric browser extension has not suffered any tampering, the biometric service creates an HTTPS connection with the appropriate web server and communicates the authentication token to the web server. The web server then validates the authentication token and completes the transaction.

[0040] In a particular embodiment, an agent application generates the display window to the user that provides transaction details and requests that the user confirm the transaction details by providing biometric authorization. This agent application is monitored by the biometric service to detect any modification of (or tampering with) the information displayed in the displayed window.

[0041] When a user begins using a device that has an associated biometric sensor, the user enrolls with the biometric user authentication system by binding their user credentials with the user's biometric template (a "fingerprint template" in specific implementations). The biometric template contains information related to the user's biometric characteristics (also referred to as "biometric information") obtained from a biometric sensor that scans or reads the user's biometric characteristics, such as a fingerprint. A user identification process identifies a particular user among multiple enrolled users (e.g., multiple users enrolled with a particular device, system or biometric sensor). A user verification process verifies that the user who provided their biometric information is who they claim to be by comparing the user's biometric information with the biometric template obtained during enrollment of the user. The enrollment, identification and verification of users are discussed in greater detail herein.

[0042] During an example enrollment process that uses a fingerprint sensor as the biometric sensor, a user swipes their finger across the fingerprint sensor several times to create a fingerprint template. The fingerprint template contains qualitative fingerprint information that allows the user's fingerprint to be distinguished from fingerprints associated with other users. In alternate embodiments, a placement fingerprint sensor (also referred to as a static fingerprint sensor) is used such that a user places their finger on the fingerprint sensor rather than "swiping" their finger across the fingerprint sensor. After creating a fingerprint template, the user provides user credentials, such as a password, cryptographic key, random seed, and the like. The systems and procedures described herein bind the user's fingerprint template with the user credentials. The fingerprint template and user credentials are then stored in a secure storage device. In one embodiment the secure storage device is contained within the fingerprint sensor hardware. In other embodiments, the secure storage device is contained in a device that utilizes the fingerprint sensor.

[0043] During an example user identification process (also referred to as a user verification process), a user swipes their finger across a fingerprint sensor. The process then determines whether the user's fingerprint information matches a fingerprint template associated with the fingerprint sensor. If the user's fingerprint information matches a fingerprint template, the user's credentials are released to the user and/or a

service or process requesting the user verification. Thus, the user credentials are not released from the secure storage device until a matching fingerprint template is confirmed. In particular embodiments, the user credentials released as a result of a match with a fingerprint template are not necessarily the same credentials provided by the user during the enrollment process. For example, the user credentials released after finding a matching fingerprint template may include an OTP (One Time Password) token, RSA signature and the like. The enrollment process can be initiated by a Web server, a Web browser plug-in, and the like.

[0044] The described systems and methods communicate user credentials to a specific address, location, or other recipient identifier. Thus, even if an imposter can gain access to the user credentials, the system will send those user credentials to a predetermined address or location, thereby preventing the imposter from attempting to have the user credentials sent to an alternate address or location. The address or location information is stored within the user credentials and is established as part of the enrollment process.

[0045] Particular embodiments of the systems and methods discussed herein use strong cryptographic algorithms implemented in hardware and/or software. Example cryptographic algorithms include AES (Advanced Encryption Standard) **256**, SHA (Secure Hash Algorithm) **256** and RSA **2048**. Example biometric sensors are compatible with various standards, such as OATH-OCRA (OATH Challenge/Response Algorithms), TOPT (Time-based One-time Password Algorithm), HOPT (HMAC-Based OTP Algorithm), PKCS (Public Key Cryptography Standards) #**11**, RSA SecureID based OTP, and the like.

[0046] In a particular implementation, each biometric sensor has a unique identifier (ID) that is used to strengthen the level of security provided by the system or process. This unique ID provides an additional authentication factor representing "something you have". Since each biometric sensor has a unique ID, each user's biometric template and user credentials can be uniquely associated with a specific biometric sensor.

[0047] Specific implementations include a biometric sensor as part of a multi-component or multi-element authentication system. Particular embodiments may include one or more authentication factors, such as: 1) something you are; 2) something you have; and 3) something you know.

[0048] The systems and methods described herein are useful in performing Web site authentication. In example embodiments, a Web site that supports the authentication procedures discussed herein includes an HTML (Hyper Text Markup Language) tag that identifies a Web browser plug-in (also referred to as a "biometric plug-in") that is installed on the user's computing device. This HTML tag indicates to the browser that the Web site supports biometric authentication. Other example embodiments include an extension of an existing Web browser plug-in. Further implementations may utilize a browser helper object, ActiveX control, Browser Extension, or other approaches. In particular implementations, the Web browser plug-in obtains the biometric sensor's unique ID and communicates that unique ID (or a hash of the unique ID) to a web server via HTTP or HTTPS.

[0049] When a user accesses the Web site, the Web browser plug-in is activated and detects that a biometric sensor is installed in the user's computing device. The Web site suggests that the user enroll with their biometric sensor to provide a more secure user authentication. If the user accepts, the Web site generates a secret key and passes the secret key to the user's computing device via a secure connection between the Web site and the user's computing device. The Web browser plug-in then activates the enrollment process to enroll the user. This enrollment process includes binding the Web site to the specific user. The web site then generates a secret key and passes the secret key to the user's computing device via a secure connection between the Web site and the user's computing device. In a particular implementation, the "enrollment" process includes enrolling the user's fingerprint and generating a secure key.

[0050] If the user also wants to bind their computing device with Web site authentication, the Web browser plug-in sends the biometric sensor's ID to the Web site server or other device/system. Multiple embodiments store information in various formats and on various devices or components within a system. Example embodiments may utilize a hash of the shared secret, a hash of the biometric sensor ID, and the like. At this point, the user can select different factors for authentication. In a particular embodiment, the Web site may require stronger authentication when an important operation is being performed on the Web site, such as accessing a bank account or other sensitive data.

[0051] After a user has enrolled with a particular Web site that supports biometric authentication, subsequent visits to the same Web site cause the Web browser plug-in to detect that the user has already enrolled with the Web site. In this situation, the Web site prompts the user to perform user authentication (e.g., using the biometric device). In the case of a fingerprint sensor, the user swipes their finger across the fingerprint sensor or places their finger on the fingerprint sensor. If the fingerprint information matches a fingerprint template associated with the fingerprint sensor, the Web browser plug-in releases user secrets from the user credentials. In particular embodiments, the fingerprint sensor releases an OTP token or an RSA signature instead of plaintext credentials. After the credentials are released, they are communicated to the Web site to complete the user authentication process. In specific implementations, the server may generate a random challenge and communicate that challenge to the client device. The Web browser plug-in (or the biometric sensor) uses this challenge to construct a response based on the secure key and the random challenge. The response may be a hash of the secure key, a hash of the random challenge, or any other calculation. The server validates the user credentials and authenticates the user if the validation is successful.

[0052] In particular implementations, the user performs the enrollment process for each Web site the user accesses that supports biometric authentication. Additionally, different user credentials are associated with each Web site with which the user enrolls. Thus, if the user enrolls with five different Web sites that support biometric authentication, the biometric sensor in the user's computing device stores five separate sets of user credentials, each of which is associated with one of the five different Web sites. Additionally, if different users access the same Web site, separate user credentials and separate biometric templates are maintained for each user.

[0053] Particular embodiments of the Web browser plug-in support WBF (Windows Biometric Framework), thereby supporting any biometric device that supports the WBF interface. The Web browser plug-in also supports the Application Programming Interface specified by the BioAPI Consortium.

[0054] In alternate embodiments, the systems and methods determine that a Web site supports biometric authentication by providing a service or process that monitors Web site data and detects certain types of transactions on secure web sites. When a secure transaction is initiated, the systems and methods check the computing device accessing the Web site to determine if the computing device includes a fingerprint sensor or other biometric device. If so, an enrollment and/or authentication process is activated to offer an enhanced level of security to the user, as described herein.

[0055] FIG. **8** shows an example system **800** capable of performing biometric user enrollment and authentication via a biometric sensor **804** (such as a fingerprint sensor or other biometric device). In this example, a biometric service **810** executes on a host PC **802** and communicates with one or more applications **812** that may request user authentication. Example applications include Internet browser applications, financial applications, and the like. In a particular embodiment, the biometric service uses a Windows API (e.g., a WinUSB Driver) **808** to encrypt a fingerprint template database with system account credentials. In alternate embodiments, any type of API or similar interface may be used in place of Windows API **808**. Biometric sensor **804** has a unique 128 bit encryption key and a unique identifier (e.g., serial number). The enrolled credentials of a user are encrypted with the encryption key and stored in a storage device, such as secure storage **806**. In a particular embodiment, biometric service **810** is implemented as a service application running in a local system account.

[0056] In a particular embodiment, application **812** is an Internet browser application executing on host PC **802** and communicating with various web servers via the Internet. Application **812** includes a browser extension or browser plug-in that communicates with biometric service **810**. In one implementation, biometric service **810** is a secure application executing in a background mode on host PC **802**. Thus, biometric service **810** provides a communication interface to biometric sensor **804**. The browser extension (or browser plug-in) associated with application **812** is capable of communicating transaction details, random challenges, signature information, user information, and other data to biometric service **810**. Biometric service **810** also communicates with one or more web servers as part of the user enrollment and/or user authentication procedure.

[0057] FIG. **9** shows another example system **900** capable of performing biometric user enrollment and authentication via a biometric sensor **904**. System **900** includes a host PC **902**, a WinUSB driver **910**, a biometric service **912** and an application **914** similar to the components discussed above with respect to FIG. **8**. In the example of FIG. **9**, the biometric sensor decrypts the user credentials only after a successful biometric reading, such as a fingerprint swipe or fingerprint scan (using a placement style fingerprint sensor). For example, in a successful fingerprint swipe, the swiped fingerprint information matches a fingerprint template associated with the fingerprint sensor. In a particular embodiment, the validity enterprise sensor has a unique 256 bit encryption key **908** and a unique identifier (e.g., serial number). The biometric sensor **904** creates a secure communication with Host PC **202** using SSL v3 protocol or other secure communication technique. In a particular implementation, biometric sensor **904** includes a "match on chip" functionality that releases a user's credentials only upon a successful fingerprint swipe or other biometric reading. User credentials and other information may be stored within biometric sensor **904**, in a secure storage **906**, or any other storage mechanism. In certain embodiments, the validity biometric service is implemented as a service application running in a local system account.

[0058] FIG. **10** shows an example user enrollment process in which the user enrolls using a fingerprint sensor to bind the user's fingerprint template with the user's credentials. An application **1004** that desires to enroll a user with a biometric device communicates with a biometric service **1002**, which is coupled to a secure storage **1006**. Biometric service **1002** is also coupled to a biometric sensor (not shown), which captures biometric data and communicates that data to the biometric service. Application **1004** initiates the user enrollment process by displaying a request **1008** for the user to provide their fingerprint (in the case of a fingerprint sensor) and provide user credentials. Application **1004** communicates a user enrollment request to biometric service **1002** as well as information regarding a user identifier (user id), an application identifier, and user credentials. The biometric service then captures the fingerprint data and stores the fingerprint data in secure storage **1006**. Additional details regarding the user enrollment process are provided herein.

[0059] FIG. **11** shows an example user authentication process using a fingerprint sensor. An application **1104** that desires to authenticate a user with a biometric device communicates with a biometric service **1102**, which is coupled to a secure storage **1106**. Biometric service **1102** is also coupled to a biometric sensor (not shown), which captures biometric data and communicates that data to the biometric service. Application **1104** initiates the user authentication process by displaying a request **1108** for the user to provide their fingerprint (in the case of a fingerprint sensor). Application **1104** communicates an authentication and/or identity request to biometric service **1102**. The biometric service then captures the fingerprint data and identifies user credentials for the user associated with the fingerprint data. The user credentials are then communicated to application **1104**. Additional details regarding the user authentication process are provided herein.

[0060] FIG. **12** shows another example system **1200** capable of performing biometric user enrollment and authentication using any number of different types or brands of fingerprint sensors. Depending on the fingerprint sensor type and/or manufacturer, the system of FIG. **12** uses: 1) a WBF (Windows Biometric Framework) interface; 2) a biometric service; or 3) any other system or service to communicate data between an Internet browser application and the fingerprint sensor.

[0061] System **1200** includes a browser application **1202** capable of communicating with a web server **1204** and a biometric service **1208**. Browser application **1202** includes a biometric extension **1218** that facilitates communication and handling of biometric-related data. In alternate embodiments, biometric extension **1218** is replaced with a browser application plug-in. Web server **1204** is coupled to a secure database **1206** that stores various data, such as data used during the biometric user enrollment and authentication procedures, as discussed herein.

[0062] Biometric service **1208** communicates with a Windows biometric framework **1210** and a fingerprint sensor **1212**. Windows biometric framework **1210** also communicates with a fingerprint sensor **1216** that is not able to communicate directly with biometric service **1208**. Thus, Windows biometric framework **1210** provides an interface between fingerprint sensor **1216** and biometric service **1208**.

Fingerprint sensor **1212** is capable of communicating directly with biometric service **1208** without needing Windows biometric framework **1210**. Fingerprint sensor **1212** is coupled to a secure storage **1214** that stores user credentials, an encryption key, and related data.

[0063] During operation of system **1200**, web server **1204** sends a web page (e.g., an HTML page) and a random challenge to browser application **1202**. Biometric extension **1218** communicates the random challenge to biometric service **1208**, which requests a response from fingerprint sensor **1212** (or requests a response from fingerprint sensor **1216** via Windows biometric framework **1210**). Fingerprint sensor **1212** sends a response to biometric service **1208** after a valid fingerprint swipe (or scan). Thus, if a user fails to swipe a finger or fingerprint sensor **1212** reads invalid fingerprint information, no response is sent to biometric service **1208**. In alternate embodiments, fingerprint sensor **1212** sends an "invalid fingerprint" message to biometric service **1208** if the fingerprint sensor reads invalid fingerprint information. If biometric service **1208** receives a positive response from fingerprint sensor **1212** (e.g., a valid fingerprint swipe), the biometric service communicates a response to the random challenge to web server **1204** using a secure communication link. Additional details regarding biometric user enrollment and authentication are provided below.

[0064] In a particular embodiment, a secret key (also referred to as a "secure key") is generated by a web server and stored by the web server. The secret key is also provided to the biometric sensor and/or the system containing the biometric sensor, and stored along with the biometric template associated with the user. The secret key can be a cryptographic key (DES, AES, etc.), a random seed, a random number, an RSA private key, and so forth. In alternate embodiments, the secret key is generated by a client device and communicated to the web server. The secure key may be transferred using HTTP or HTTPS and can be transferred directly to the browser application or directly to the browser application plug-in (or browser application extension). The biometric template is typically generated during enrollment of the user. Additionally, if the biometric device has a unique ID, that unique ID is sent to the web server for storage and use in future authentication procedures.

[0065] In particular embodiments, binary files used in the systems and methods discussed herein are signed and authenticated prior to running the binary files. This approach blocks malicious attempts to replace or edit the binary files. Additionally, applications communicating with the biometric service are validated at runtime.

[0066] FIG. **13** is a flow diagram depicting an embodiment of a procedure **1300** for enrolling a user of a biometric authentication system. Initially, procedure **1300** detects a finger contacting a fingerprint sensor or other biometric sensor (block **1302**). Fingerprint information is read as the user swipes their finger across the fingerprint sensor (block **1304**). In alternate embodiments using a placement fingerprint sensor, the fingerprint information is scanned as the user positions their finger on the sensor. The procedure continues by creating a fingerprint template associated with the fingerprint information (block **1306**).

[0067] Procedure **1300** receives user credentials associated with the user (block **1308**). Example user credentials include a password, a cryptographic key, a random seed or any other similar confidential information. Next, the procedure binds the user credentials with the fingerprint template (block **1310**), then stores the user credentials and the fingerprint template (block **1312**) in a secure storage device.

[0068] In a specific embodiment, the procedure also binds a particular web site (e.g., a web site requesting biometric enrollment and/or biometric authentication of a user) with the fingerprint template. Thus, a particular user may perform the biometric enrollment procedure for each web site that the user is to provide future biometric authorization or biometric authentication.

[0069] FIG. **14** is a flow diagram depicting an embodiment of a procedure **1400** for authenticating a user of a biometric authentication system. Procedure **1400** is performed after a particular user has enrolled with the biometric authentication system using, for example, the procedure discussed with respect to FIG. **13**. The authentication procedure reads fingerprint information from a user's finger in contact with a fingerprint sensor (block **1402**). Procedure **1400** then identifies a fingerprint template associate with the user (block **1404**) who is accessing the fingerprint sensor. The fingerprint information read from the user's finger is compared with the fingerprint template (block **1406**) to determine whether there is a match (block **1408**). If the fingerprint information read by the fingerprint sensor does not match the information stored in the fingerprint template, the biometric authentication system does not retrieve the user credentials (block **1414**). Thus, the user credentials remain securely stored if a match is not detected.

[0070] If the fingerprint information read by the fingerprint sensor matches the information stored in the fingerprint template, the biometric authentication system retrieves the credentials associated with the user (block **1410**). The user credentials are then communicated to a requesting process or system (block **1412**).

[0071] FIG. **15** is a flow diagram depicting another embodiment of a procedure **1500** for authenticating a user of a biometric authentication system. Initially, procedure **1500** reads fingerprint information from a user's finger in contact with a fingerprint sensor (**1502**). The procedure then authenticates the fingerprint information (block **1504**). If the fingerprint information is not authenticated, a message is generated indicating an authentication failure (block **1506**). If the fingerprint information is authenticated, the procedure retrieves credentials associated with the user based on the fingerprint information (block **1508**). The procedure then decrypts the user credentials (block **1510**) and identifies a unique identifier associated with the fingerprint sensor (block **1512**). The decrypted credentials and the unique identifier are communicated to a requesting process or system (block **1514**).

[0072] FIG. **16** is a flow diagram depicting an embodiment of a procedure **1600** for authenticating a user of a Web browser application that supports biometric authentication. Initially, a web browser application accesses a web site that supports biometric authentication (block **1602**). The procedure then determines whether a biometric device is installed in the system executing the web browser application (block **1604**). The biometric device may be physically installed in the system or coupled to the system, such as via a universal serial bus (USB) or other communication link. If a biometric device is not installed (block **1606**), the web browser application operates without biometric authentication (block **1614**).

[0073] If a biometric device is installed in the system executing the web browser application, the web browser application offers enhanced security to a user through the use

of the biometric device (block **1608**). If the user accepts the offer of enhanced security at block **1610**, the user enrolls using the biometric device (block **1612**). The user enrolls, for example, using the enrollment procedure discussed herein. If the user does not accept the offer of enhanced security at block **1610**, the web browser application operates without biometric authentication (block **1614**).

[0074] FIG. **17** depicts another embodiment of a procedure for enrolling a user of a biometric authentication system. FIG. **17** shows the various actions and functions performed during the enrollment of a user and the component or system that performs those actions or functions.

[0075] FIG. **18** depicts another embodiment of a procedure for identifying and authenticating a user of a biometric authentication system. FIG. **18** shows the various actions and functions performed during the identification and authentication of a user and the component or system that performs those actions or functions.

[0076] The invention may also involve a number of functions to be performed by a computer processor, such as a microprocessor. The microprocessor may be a specialized or dedicated microprocessor that is configured to perform particular tasks according to the invention, by executing machine-readable software code that defines the particular tasks embodied by the invention. The microprocessor may also be configured to operate and communicate with other devices such as direct memory access modules, memory storage devices, Internet related hardware, and other devices that relate to the transmission of data in accordance with the invention. The software code may be configured using software formats such as Java, C++, XML (Extensible Mark-up Language) and other languages that may be used to define functions that relate to operations of devices required to carry out the functional operations related to the invention. The code may be written in different forms and styles, many of which are known to those skilled in the art. Different code formats, code configurations, styles and forms of software programs and other means of configuring code to define the operations of a microprocessor in accordance with the invention will not depart from the spirit and scope of the invention.

[0077] Within the different types of devices, such as laptop or desktop computers, hand held devices with processors or processing logic, and also possibly computer servers or other devices that utilize the invention, there exist different types of memory devices for storing and retrieving information while performing functions according to the invention. Cache memory devices are often included in such computers for use by the central processing unit as a convenient storage location for information that is frequently stored and retrieved. Similarly, a persistent memory is also frequently used with such computers for maintaining information that is frequently retrieved by the central processing unit, but that is not often altered within the persistent memory, unlike the cache memory. Main memory is also usually included for storing and retrieving larger amounts of information such as data and software applications configured to perform functions according to the invention when executed by the central processing unit. These memory devices may be configured as random access memory (RAM), static random access memory (SRAM), dynamic random access memory (DRAM), flash memory, and other memory storage devices that may be accessed by a central processing unit to store and retrieve information. During data storage and retrieval operations, these memory devices are transformed to have different states, such as different electrical charges, different magnetic polarity, and the like. Thus, systems and methods configured according to the invention as described herein enable the physical transformation of these memory devices. Accordingly, the invention as described herein is directed to novel and useful systems and methods that, in one or more embodiments, are able to transform the memory device into a different state. The invention is not limited to any particular type of memory device, or any commonly used protocol for storing and retrieving information to and from these memory devices, respectively.

[0078] Embodiments of the systems and methods described herein facilitate enrollment and authentication of users through a biometric device, such as a fingerprint sensor. Certain embodiments described herein facilitate one or more secure transactions. Additionally, some embodiments are used in conjunction with one or more conventional fingerprint sensing systems and methods. For example, one embodiment is used as an improvement of existing fingerprint detection and/or sensing systems.

[0079] Although the components and modules illustrated herein are shown and described in a particular arrangement, the arrangement of components and modules may be altered to enroll and authenticate users in a different manner, or to implement secure transactions in a different manner. In other embodiments, one or more additional components or modules may be added to the described systems, and one or more components or modules may be removed from the described systems. Alternate embodiments may combine two or more of the described components or modules into a single component or module.

[0080] Although specific embodiments of the invention have been described and illustrated, the invention is not to be limited to the specific forms or arrangements of parts so described and illustrated. The scope of the invention is to be defined by the claims appended hereto and their equivalents.

1. An apparatus configured to perform a secured transaction, comprising:

a biometric sensor configured to identify biometric information associated with a user;

a storage device coupled to the biometric sensor and configured to store user information;

a biometric service coupled to the biometric sensor and configured to communicate with the biometric sensor; and

a web browser application configured in software code and stored on a client device and configured to be executed by a client processor on the apparatus, wherein the web browser application includes a biometric extension configured to communicate with the biometric sensor via the biometric service, and wherein the biometric extension is further configured to communicate with a plurality of web servers with which to perform a secured transaction, the web browser application configured to perform the following functions when executed by the client processor

receiving a user transaction request at a client device;

communicating the user transaction request to a server, wherein the server determines whether the user transaction request is a secure transaction;

receiving transaction data from the server via the web browser application;

if the received transaction data from the server indicates a secure transaction:

prompting the user to provide biometric data;

receiving biometric data from the user; and

communicating a transaction confirmation to the server with the web browser application.

2. The apparatus of claim **1**, wherein the web browser application is further configured to receive user credentials associated with the user.

3. The apparatus of claim **1**, wherein the web browser application is further configured to receive user credentials associated with the user from one of the plurality of web servers.

4. The apparatus of claim **1**, wherein the storage device is configured to store a secret key associated with the user.

5. The apparatus of claim **1**, further comprising an encryption key embedded within the biometric sensor.

6. The apparatus of claim **1**, wherein the biometric extension has an associated digital signature.

7. The apparatus of claim **1**, wherein the biometric sensor is further configured to release an authentication token to the biometric service upon authentication of the user.

8. The apparatus of claim **7**, wherein the authentication token is a secret key.

9. The apparatus of claim **7**, wherein the authentication token is a one time password.

10. The apparatus of claim **7**, wherein the authentication token is an RSA signature.

11. The apparatus of claim **1**, wherein the biometric sensor is a fingerprint sensor.

12. The apparatus of claim **11**, wherein the fingerprint sensor is a placement fingerprint sensor.

13. The apparatus of claim **11**, wherein the fingerprint sensor is a swipe fingerprint sensor.

14. A method comprising:

identifying a biometric sensor associated with a client device, wherein the biometric sensor is identified by a biometric extension associated with a web browser application;

receiving a token and a user transaction request from the biometric sensor in response to a valid user activation of the biometric sensor;

transmitting the token to a web server using the biometric extension, wherein the server determines whether the user transaction request is a secure transaction;

transmitting a user identifier associated with the user to the web server, wherein the user identifier is communicated by the biometric extension at the client device; and

transmitting a biometric sensor identifier associated with the biometric sensor to the web server using the biometric extension

transmitting a transaction confirmation to the server with the web browser application.

15. The method of claim **14**, further comprising generating a request to authenticate the user of the biometric sensor.

16. The method of claim **14**, wherein the method is initiated in response to the web browser application accessing a web site that supports biometric authentication.

17. The method of claim **16**, further comprising determining whether the user is enrolled with the web site being accessed.

18. The method of claim **14**, further comprising creating a secure communication link between the biometric extension and the web server.

19. The method of claim **14**, further comprising receiving a session identifier from the web server using the biometric extension.

20. The method of claim **14**, wherein the token is one of a secret key, a one time password, and an RSA signature.

* * * * *