



US007908645B2

(12) **United States Patent**
Varghese et al.

(10) **Patent No.:** **US 7,908,645 B2**
(45) **Date of Patent:** **Mar. 15, 2011**

(54) **SYSTEM AND METHOD FOR FRAUD MONITORING, DETECTION, AND TIERED USER AUTHENTICATION**

5,452,413 A 9/1995 Blades
5,555,365 A 9/1996 Selby et al.
5,559,961 A 9/1996 Blonder
5,572,644 A 11/1996 Liaw et al.
5,577,125 A 11/1996 Salahshour et al.
5,604,854 A 2/1997 Glassey
5,623,591 A 4/1997 Cseri

(75) Inventors: **Thomas Emmanuel Varghese**, San Mateo, CA (US); **Jon Bryan Fisher**, Tiburon, CA (US); **Steven Lucas Harris**, Foster City, CA (US); **Don Bosco Durai**, Fremont, CA (US)

(Continued)

FOREIGN PATENT DOCUMENTS

(73) Assignee: **Oracle International Corporation**, Redwood Shores, CA (US)

GB 2313460 A 11/1997
(Continued)

OTHER PUBLICATIONS

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 768 days.

International Search Report of Apr. 7, 2006 for PCT application No. PCT/US2005/024376.

(Continued)

(21) Appl. No.: **11/412,997**

Primary Examiner — David J Pearson

(22) Filed: **Apr. 28, 2006**

(74) *Attorney, Agent, or Firm* — Kilpatrick Townsend & Stockton LLP

(65) **Prior Publication Data**

US 2006/0282660 A1 Dec. 14, 2006

Related U.S. Application Data

(60) Provisional application No. 60/676,141, filed on Apr. 29, 2005.

(51) **Int. Cl.**
G06F 7/04 (2006.01)

(52) **U.S. Cl.** **726/4; 715/773; 715/830; 715/833**

(58) **Field of Classification Search** None
See application file for complete search history.

(56) **References Cited**

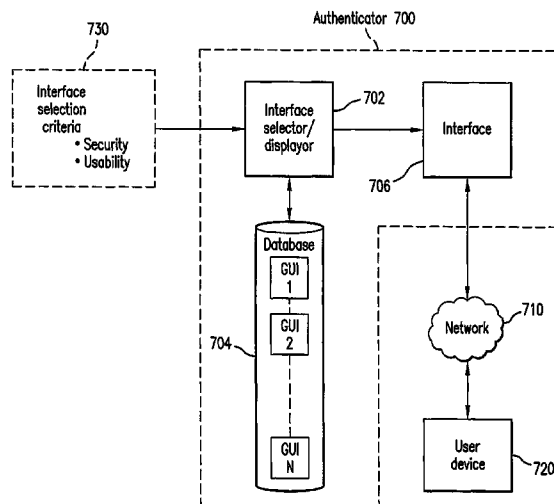
U.S. PATENT DOCUMENTS

D95,205 S 4/1935 Harrison
D298,837 S 12/1988 Thomas
5,416,895 A 5/1995 Anderson et al.
5,428,349 A 6/1995 Baker

(57) **ABSTRACT**

The present invention provides systems and methods for authenticating access requests from user devices by presenting one of a plurality of graphical user interfaces selected depending on a perceived risk of fraud associated with the devices. User devices are identified with fingerprinting information, and their associated risks of fraud are determined from past experience with the device or with similar devices and from third party information. In preferred embodiments, different graphical user interfaces are presented based on both fraud risk and, in the case of a known user, usability. In preferred embodiments, this invention is implemented as a number of communicating modules that identify user devices, assess their risk of fraud, present selected user interfaces, and maintain databases of fraud experiences. This invention also includes systems providing these authentication services.

26 Claims, 21 Drawing Sheets



U.S. PATENT DOCUMENTS

5,664,099	A	9/1997	Ozzie et al.	
5,798,760	A	8/1998	Vayda et al.	
D400,195	S	10/1998	Utesch	
5,821,933	A	10/1998	Keller et al.	
5,875,296	A	2/1999	Shi et al.	
5,928,364	A	7/1999	Yamamoto	
5,949,348	A	9/1999	Kapp et al.	
5,966,127	A	10/1999	Yajima	
D419,907	S	2/2000	Vogelbruch	
6,023,506	A	2/2000	Ote et al.	
6,064,972	A *	5/2000	Jankowitz et al.	705/7
6,111,984	A	8/2000	Fukasawa	
6,209,102	B1	3/2001	Hoover	
6,209,104	B1	3/2001	Jalili	
6,240,183	B1	5/2001	Marchant	
6,253,326	B1	6/2001	Lincke et al.	
6,263,447	B1	7/2001	French et al.	
6,282,551	B1	8/2001	Anderson et al.	
6,343,361	B1	1/2002	Nendell et al.	
6,369,839	B1	4/2002	Peterson	
6,448,987	B1	9/2002	Easty et al.	
6,658,574	B1	12/2003	Anvekar	
6,718,471	B1	4/2004	Kashima	
6,725,422	B1	4/2004	Bauchot et al.	
6,741,268	B1	5/2004	Hayakawa	
D492,691	S	7/2004	Kortis	
D493,471	S	7/2004	McIntosh	
6,853,973	B2	2/2005	Mathews et al.	
D505,135	S	5/2005	Sapp et al.	
6,895,502	B1	5/2005	Fraser	
6,934,860	B1	8/2005	Goldstein	
6,972,363	B2	12/2005	Georges et al.	
7,036,091	B1	4/2006	Nguyen	
7,082,227	B1	7/2006	Baum et al.	
7,100,049	B2	8/2006	Gasparini et al.	
7,137,008	B1 *	11/2006	Hamid et al.	713/182
D539,809	S	4/2007	Totten et al.	
7,200,747	B2	4/2007	Riedel et al.	
7,219,368	B2 *	5/2007	Juels et al.	726/2
7,240,367	B2	7/2007	Park	
7,437,024	B2	10/2008	Baum et al.	
7,523,067	B1 *	4/2009	Nakajima	705/39
7,596,701	B2	9/2009	Varghese	
7,616,764	B2	11/2009	Varghese	
2001/0027529	A1	10/2001	Sasabe et al.	
2002/0013905	A1 *	1/2002	Hamada	713/185
2002/0029341	A1	3/2002	Juels et al.	
2002/0049614	A1	4/2002	Rice et al.	
2002/0087894	A1 *	7/2002	Foley et al.	713/202
2002/0122031	A1	9/2002	Maglio et al.	
2002/0188872	A1 *	12/2002	Willeby	713/202
2003/0005329	A1	1/2003	Ikonen	
2003/0097593	A1	5/2003	Sawa et al.	
2003/0182558	A1	9/2003	Lazzaro et al.	
2003/0210127	A1	11/2003	Anderson	
2004/0010721	A1	1/2004	Kirovski et al.	
2004/0030933	A1	2/2004	Park	
2004/0030934	A1	2/2004	Mizoguchi et al.	
2004/0034801	A1	2/2004	Jaeger	
2004/0059951	A1	3/2004	Pinkas et al.	
2004/0083389	A1 *	4/2004	Yoshida	713/201
2004/0117320	A1	6/2004	Morioka et al.	
2004/0128534	A1 *	7/2004	Walker	713/200
2004/0153660	A1 *	8/2004	Gaither et al.	713/200
2004/0168083	A1	8/2004	Gasparini et al.	
2004/0215980	A1	10/2004	Hamid	
2004/0221163	A1 *	11/2004	Jorgensen et al.	713/182
2004/0230843	A1	11/2004	Jansen	
2004/0250138	A1	12/2004	Schneider	
2005/0010768	A1	1/2005	Light et al.	

2005/0015601	A1	1/2005	Tabi	
2005/0044425	A1 *	2/2005	Hypponen	713/202
2005/0097320	A1 *	5/2005	Golan et al.	713/166
2005/0144451	A1	6/2005	Voice et al.	
2005/0193208	A1	9/2005	Charrette et al.	
2005/0204131	A1 *	9/2005	Kovarik, Jr.	713/166
2005/0204145	A1	9/2005	Makishima	
2005/0251752	A1 *	11/2005	Tan et al.	715/741
2005/0278542	A1 *	12/2005	Pierson et al.	713/182
2005/0278647	A1	12/2005	Leavitt et al.	
2006/0011045	A1 *	1/2006	Yamashita et al.	84/611
2006/0020815	A1	1/2006	Varghese et al.	
2006/0104446	A1	5/2006	Varghese et al.	
2006/0212829	A1	9/2006	Yahiro et al.	
2007/0097351	A1	5/2007	York et al.	
2007/0165849	A1	7/2007	Varghese et al.	
2007/0192615	A1	8/2007	Varghese et al.	
2009/0089869	A1	4/2009	Varghese	

FOREIGN PATENT DOCUMENTS

JP	2004258845	A *	9/2004
WO	WO 96/18139	A1	6/1996
WO	WO 2004/053674	A2	6/2004
WO	WO 2006/010058	A2	1/2006
WO	WO 2006/118968	A2	11/2006
WO	WO 2007/087352	A2	8/2007

OTHER PUBLICATIONS

International Preliminary Report on Patentability of Apr. 13, 2007 for PCT application No. PCT/US2005/024376.
 Written Opinion of Apr. 7, 2006 for PCT application No. PCT/US2005/024376.
 International Search Report of Jul. 7, 2008 in corresponding international application PCT/US06/16085.
 Written Opinion of Jul. 7, 2008 in corresponding international application PCT/US06/16085.
 International Search Report of Feb. 14, 2008 in PCT application No. PCT/US07/01899.
 Written Opinion of Feb. 14, 2008 in PCT application No. PCT/US07/01899.
 International Preliminary Report on Patentability of Jan. 2, 2009 in PCT application No. PCT/US07/01899; pp. 10.
 US Non-Final Office Action for U.S. Appl. No. 11/340,376, dated Jan. 15, 2009; pp. 9.
 US Non-Final Office Action for U.S. Appl. No. 11/318,414, dated Jan. 27, 2009; pp. 8.
 International Preliminary Report on Patentability of Aug. 28, 2008 in International Application No. PCT/US2006/016085.
 Non-Final Office Action for U.S. Appl. No. 11/340,376 mailed on Aug. 4, 2008; pp. 5.
 Advisory Office Action for U.S. Appl. No. 11/340,376 mailed on May 27, 2008; pp. 3.
 Notice of Allowance for U.S. Appl. No. 11/340,376 mailed on Jun. 12, 2009; pp. 12.
 Notice of Allowance for U.S. Appl. No. 11/169,564 mailed on Jun. 1, 2009; pp. 9.
 Final Office Action for U.S. Appl. No. 11/318,424 mailed on Jun. 2, 2009; pp. 16.
 Non-Final Office Action for U.S. Appl. No. 11/318,424 mailed on Sep. 1, 2009; 14 pages.
 Final Office Action for U.S. Appl. No. 11/318,424 mailed on Mar. 10, 2010; 11 pages.
 Advisory Action for U.S. Appl. No. 11/318,424 mailed on May 25, 2010, 3 pages.
 Notice of Allowance for U.S. Appl. No. 11/318,424 mailed on Jun. 16, 2010; 7 pages.

* cited by examiner

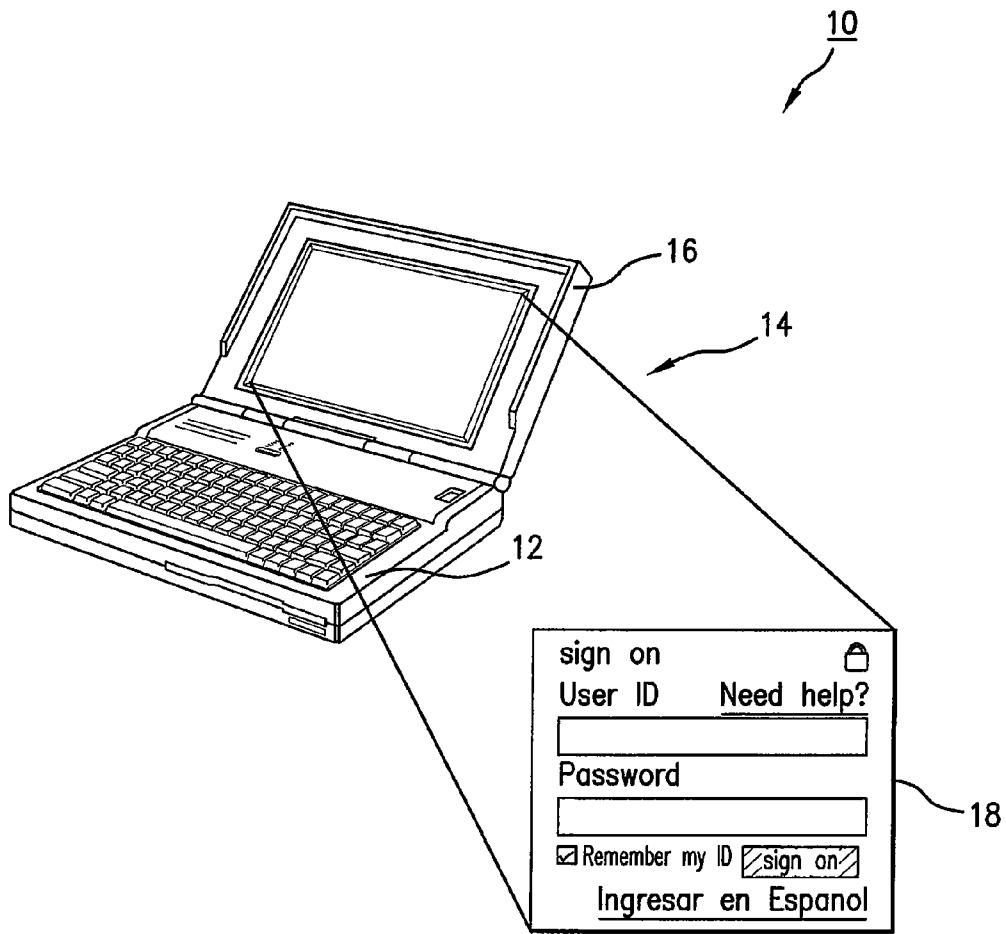


FIG. 1
PRIOR ART

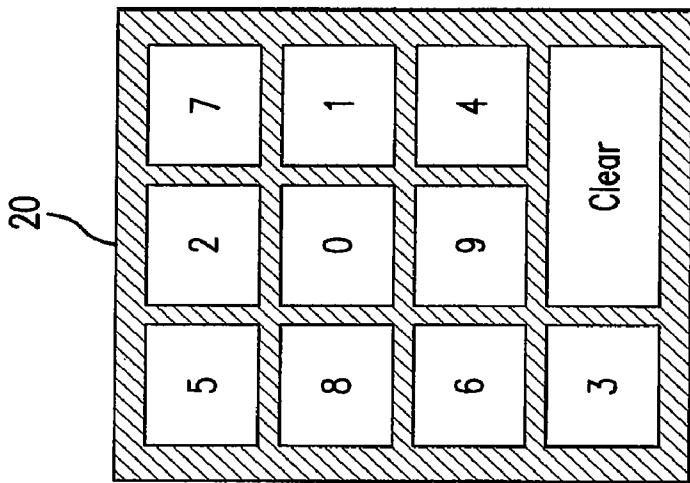


FIG. 2
PRIOR ART

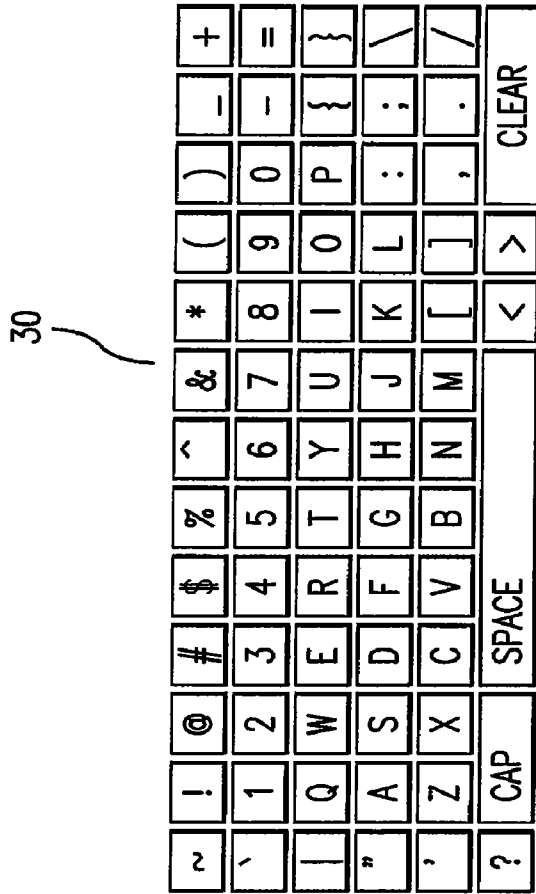


FIG. 3
PRIOR ART

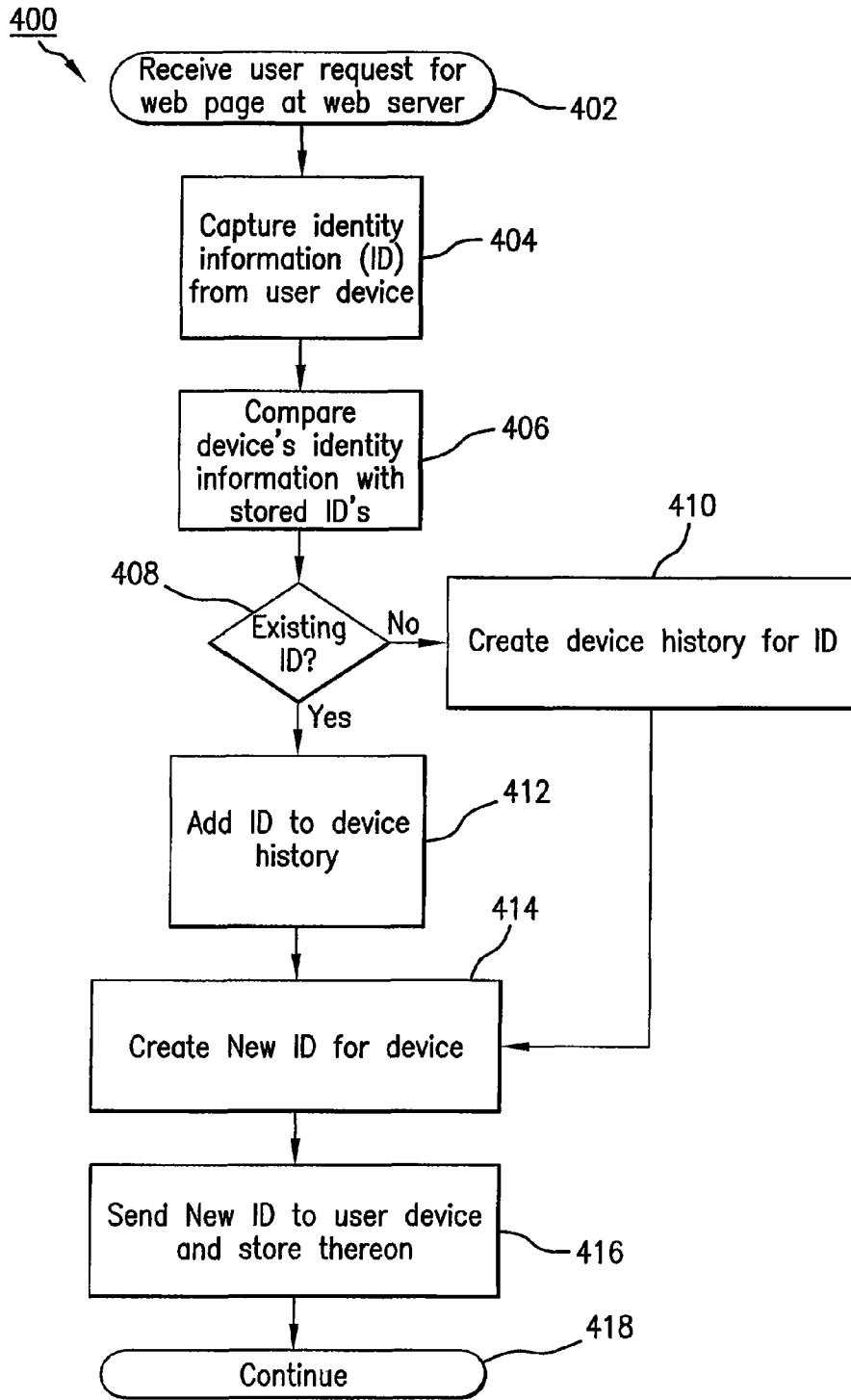


FIG.4A

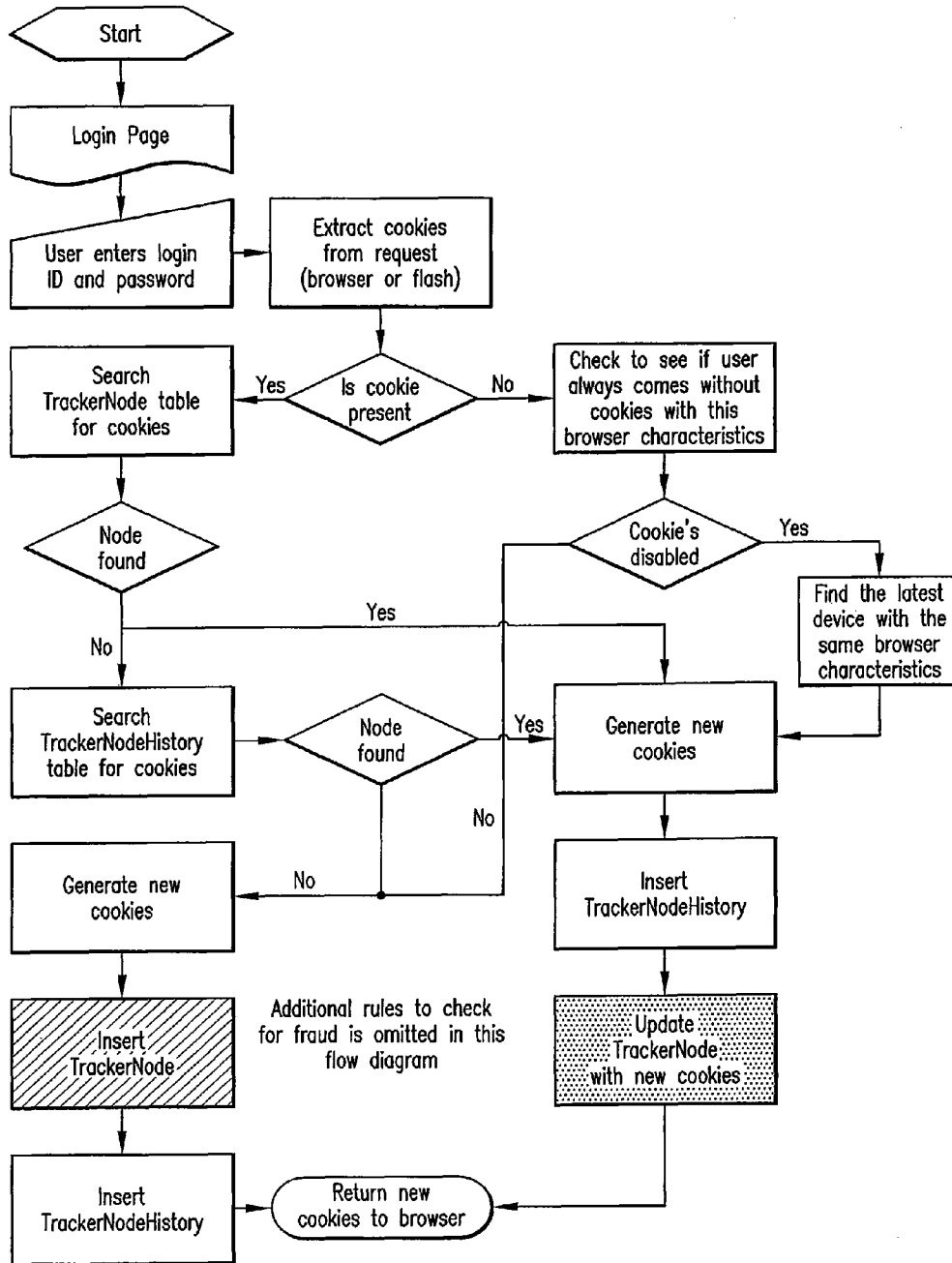


FIG. 4B

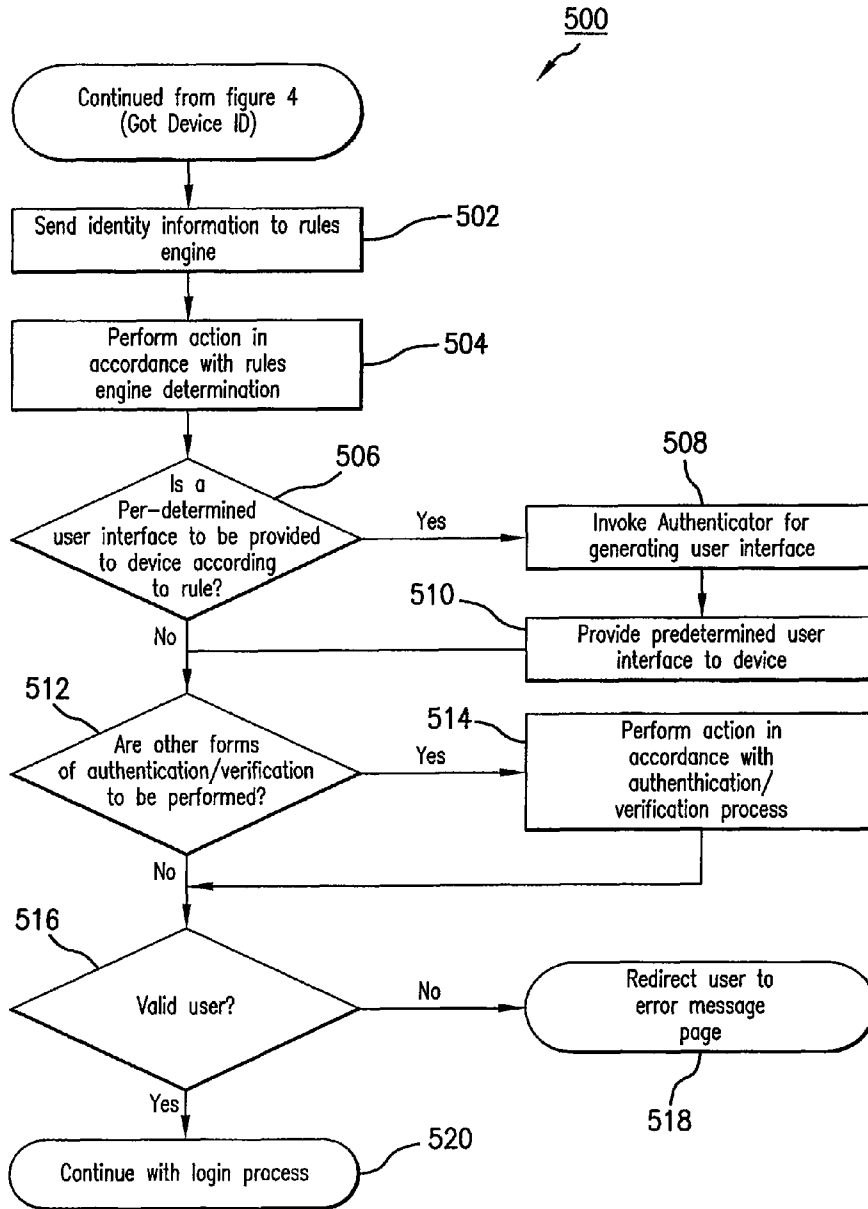


FIG.5

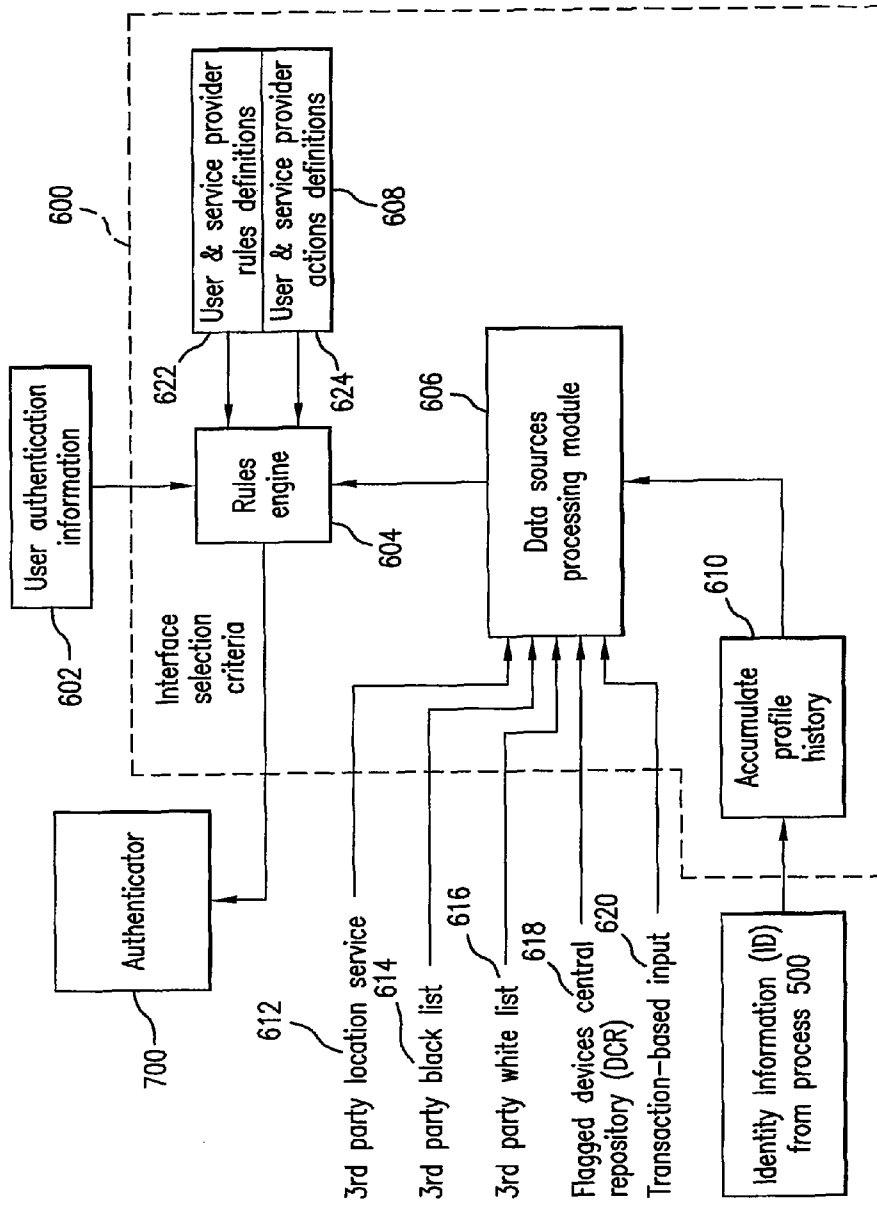


FIG. 6

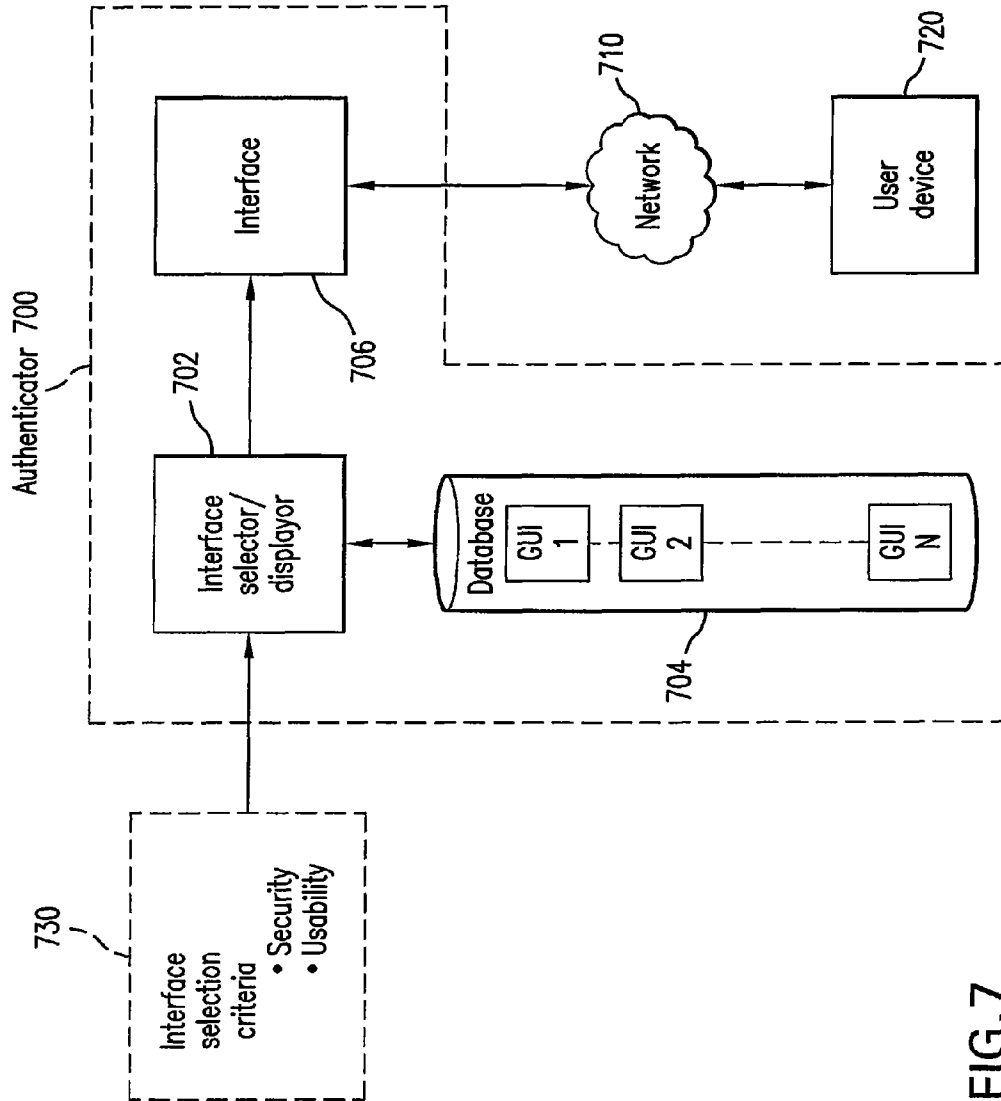


FIG. 7

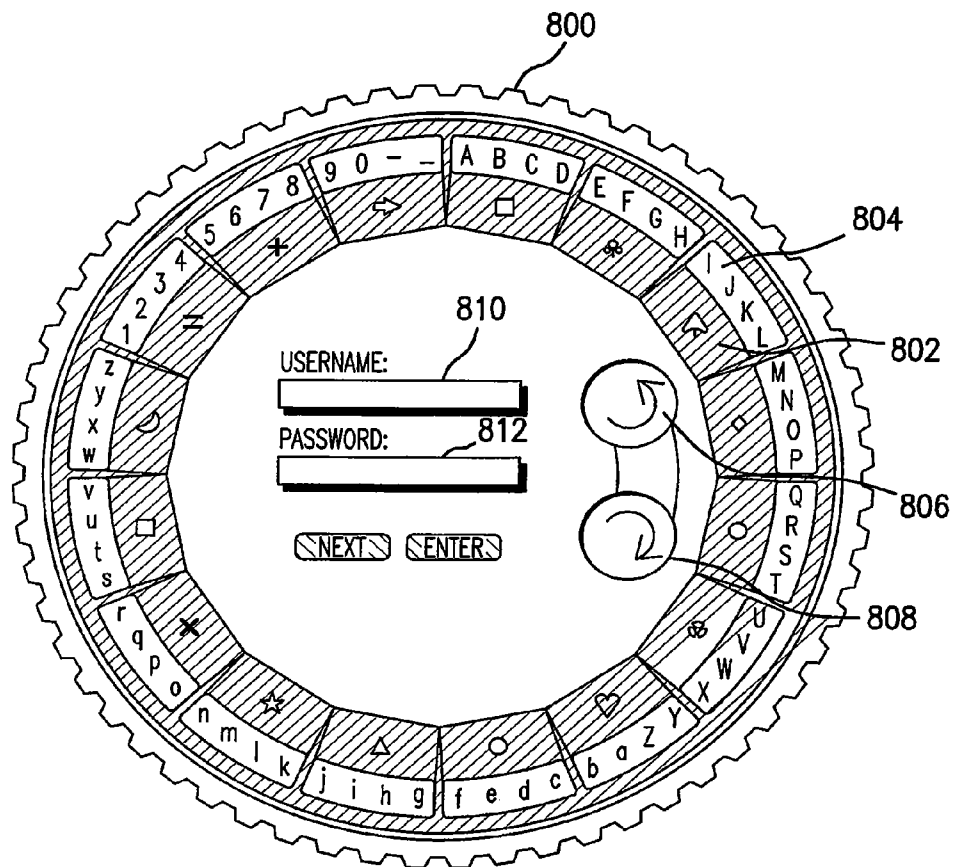


FIG. 8

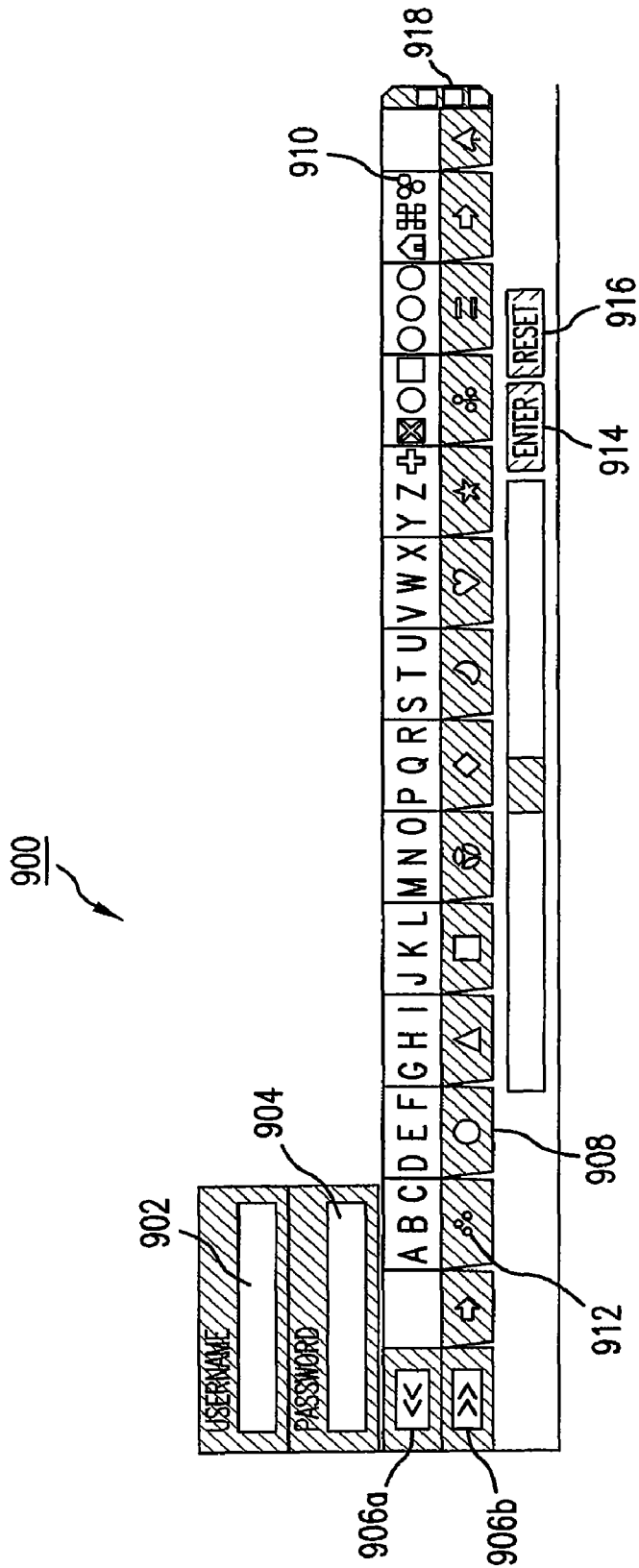


FIG. 9

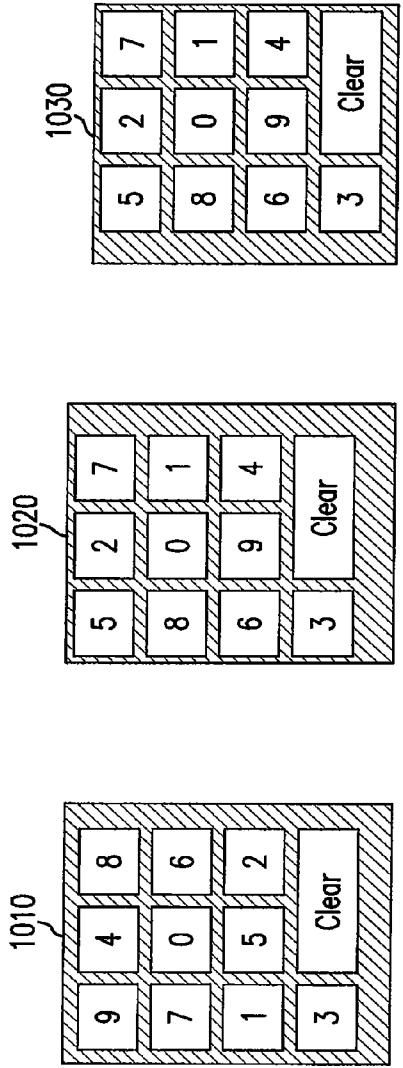


FIG. 10a

FIG. 10b

FIG. 10c

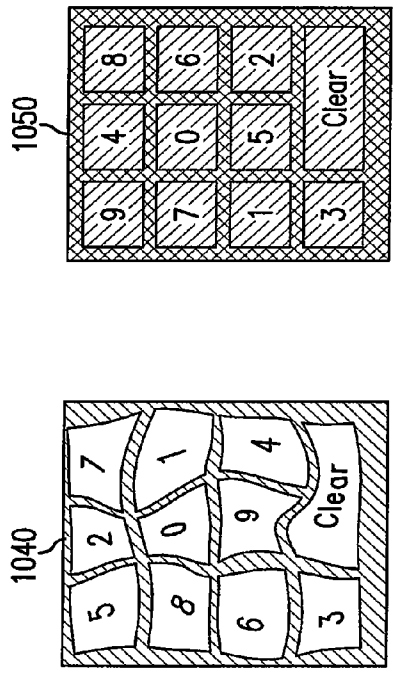


FIG. 10d

FIG. 10e

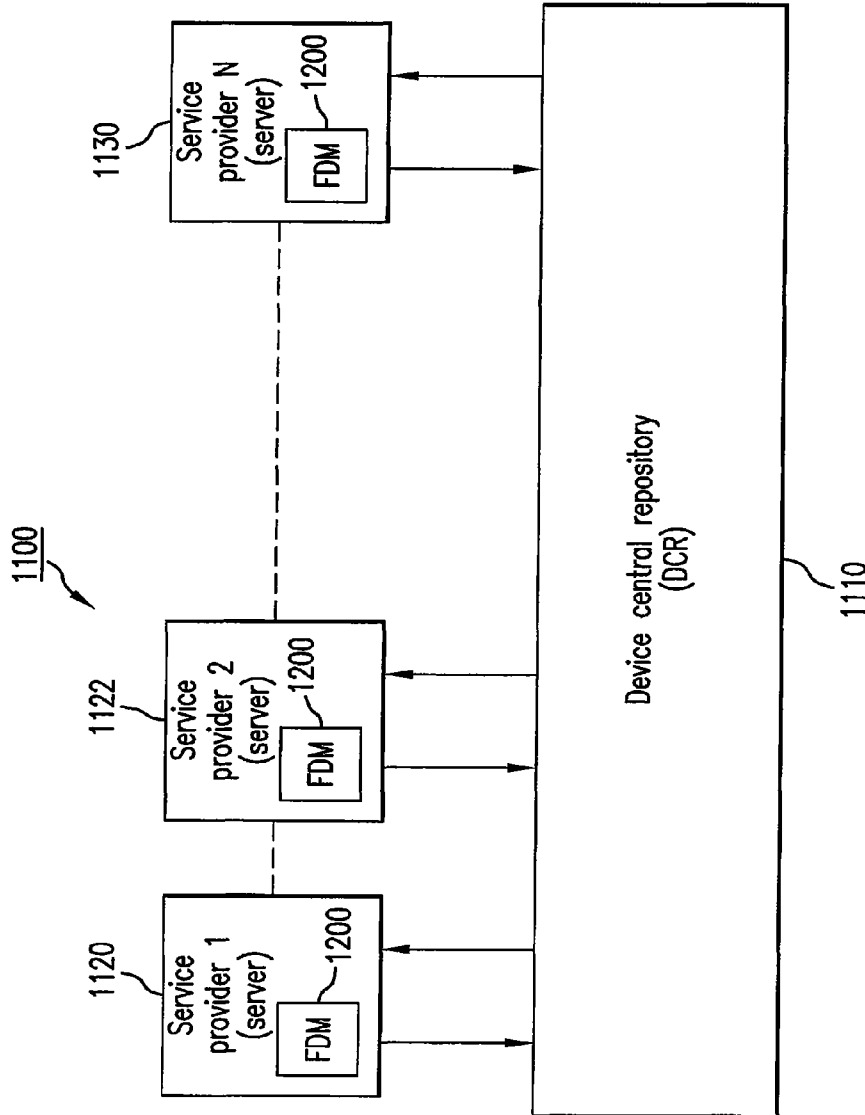


FIG. 11

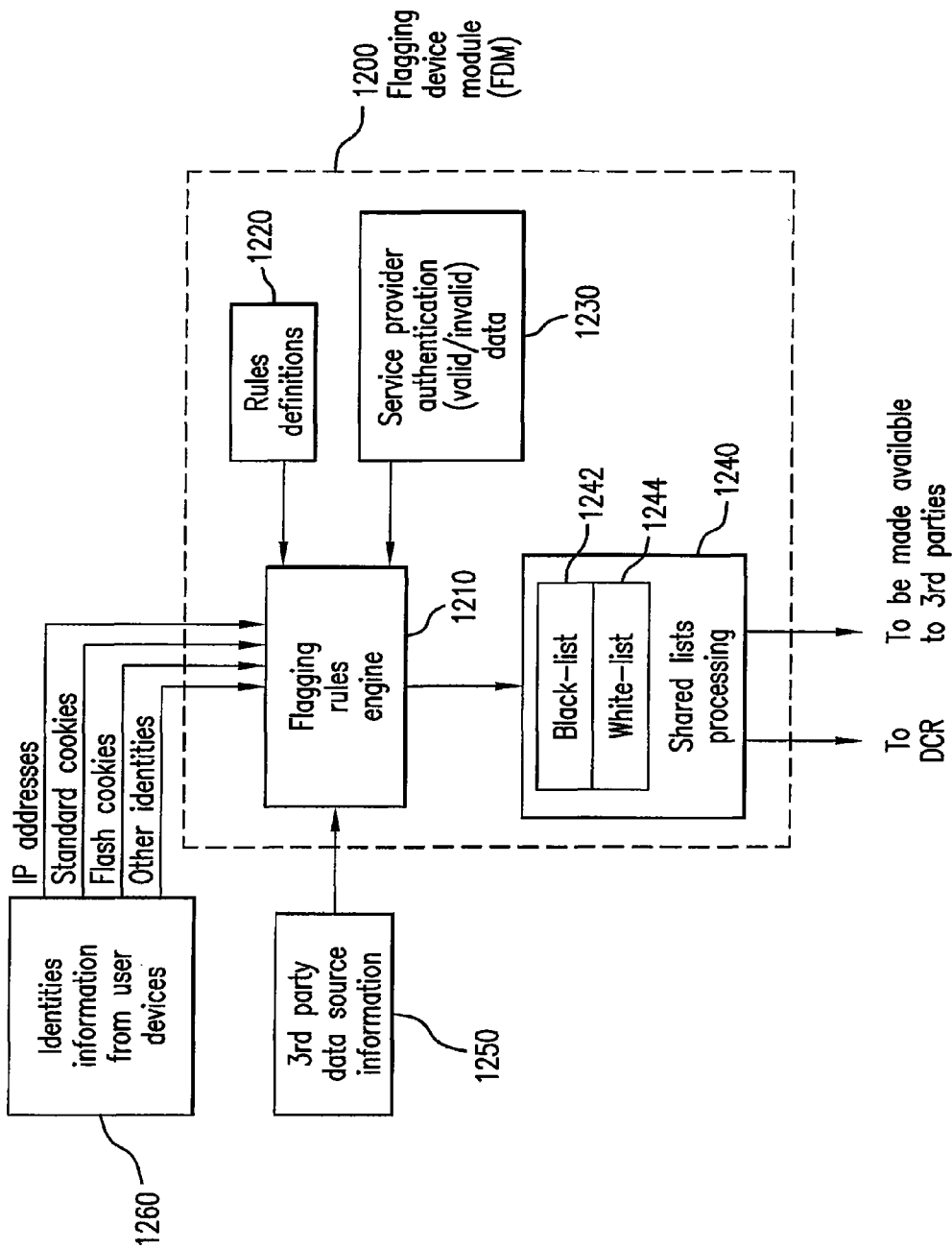


FIG. 12

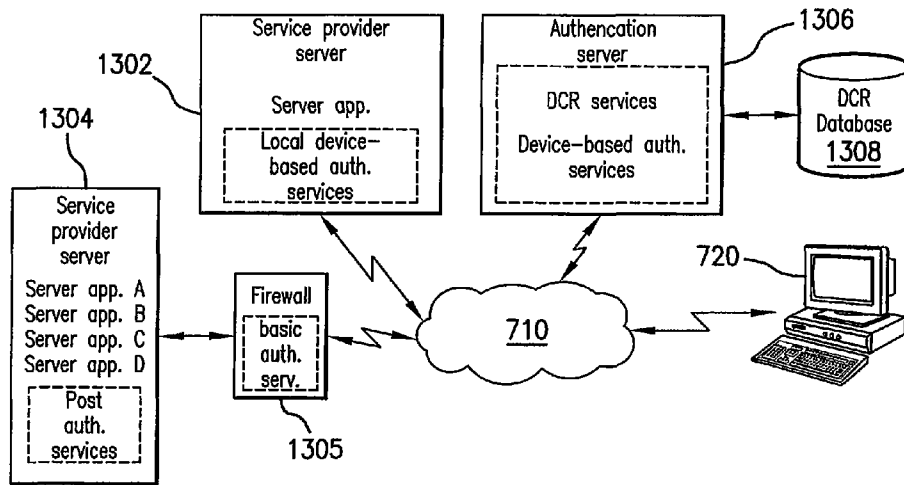


FIG. 13A

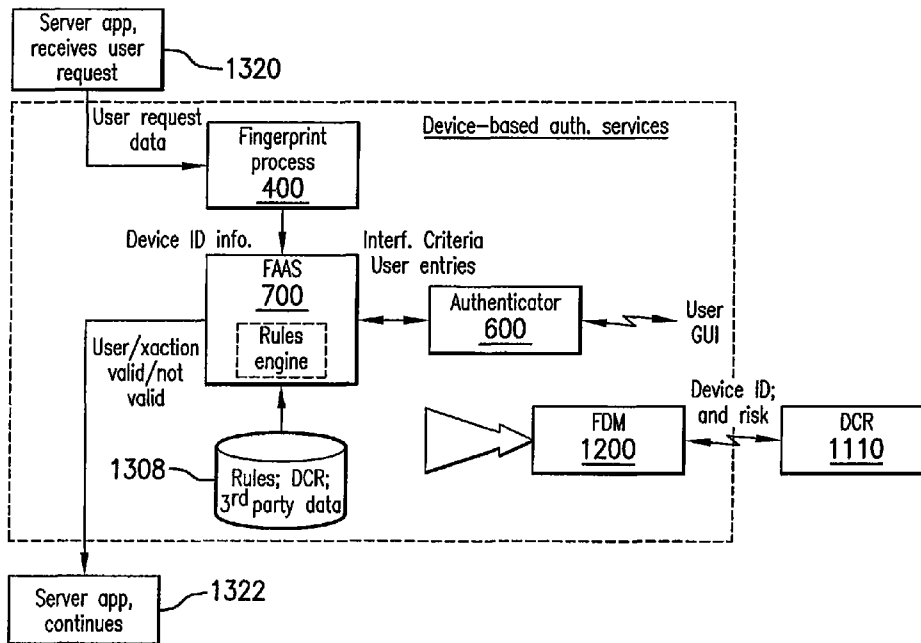


FIG. 13B

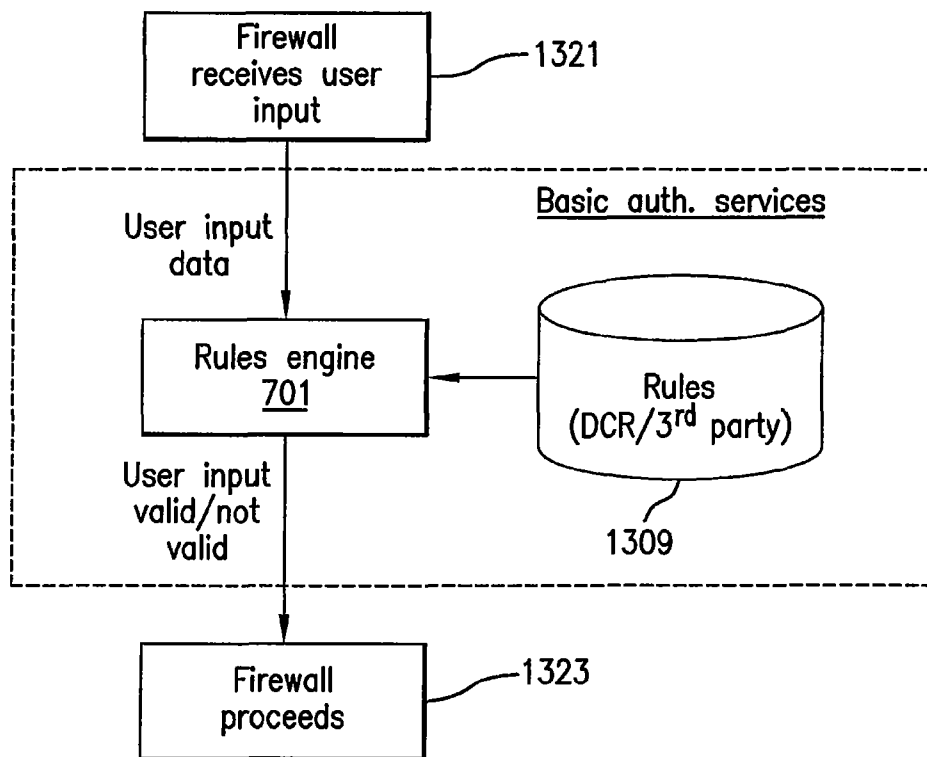


FIG. 13C

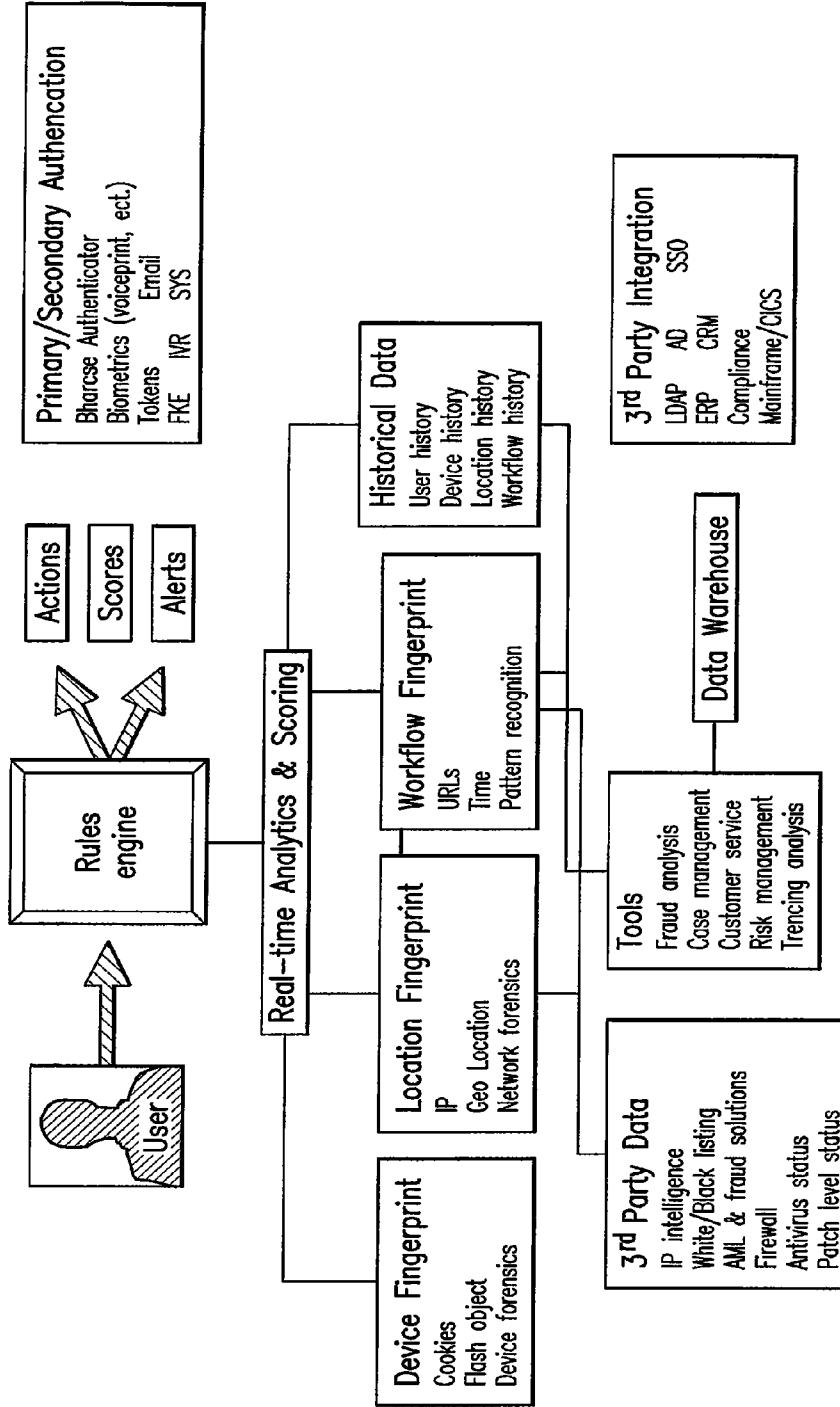


FIG. 14

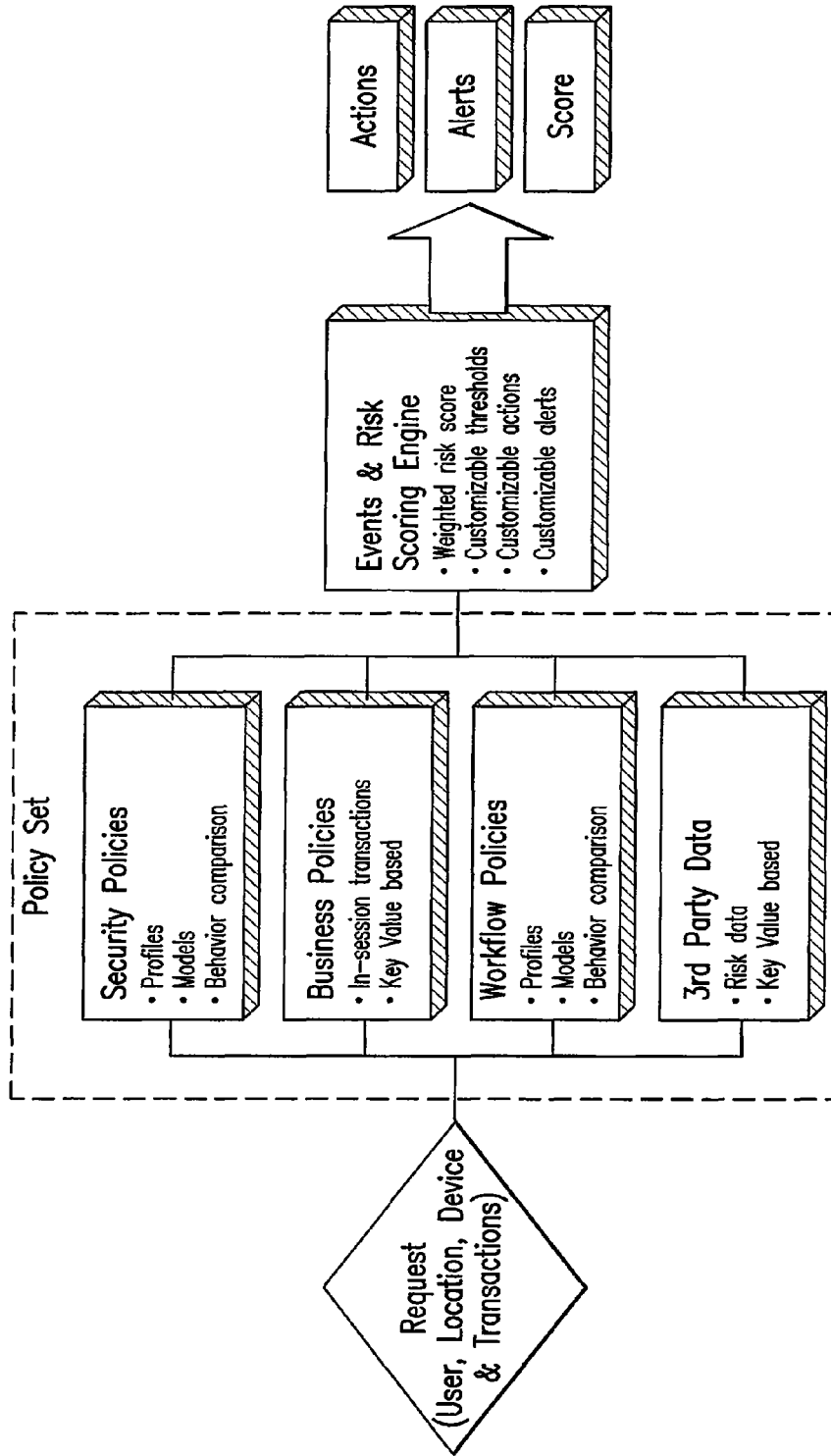


FIG. 15A

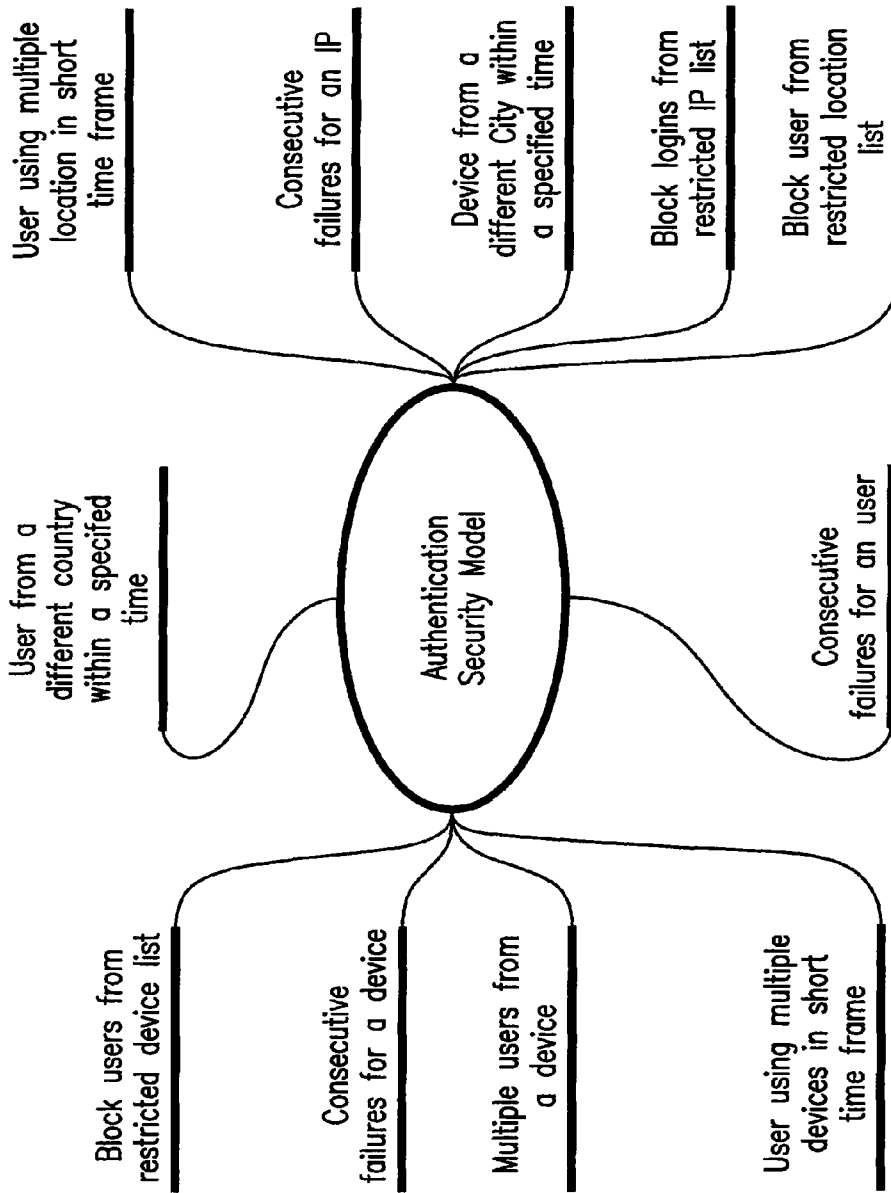


FIG. 15B

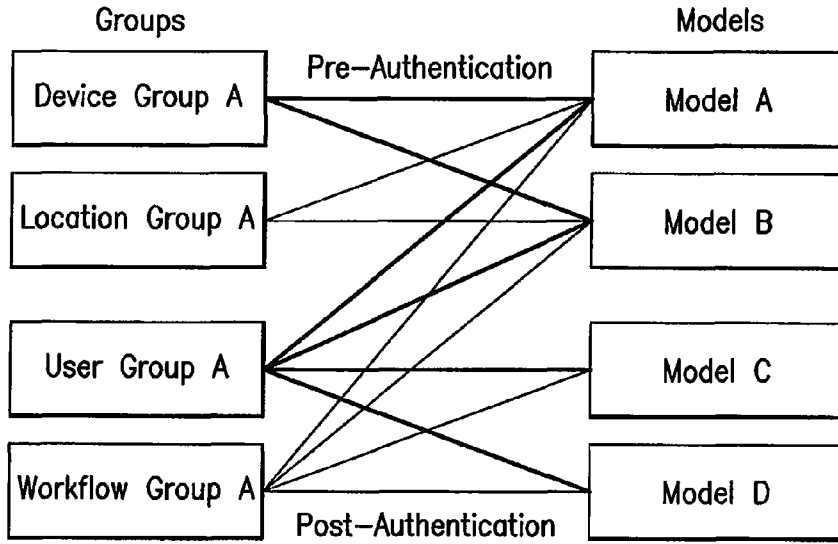


FIG. 16A

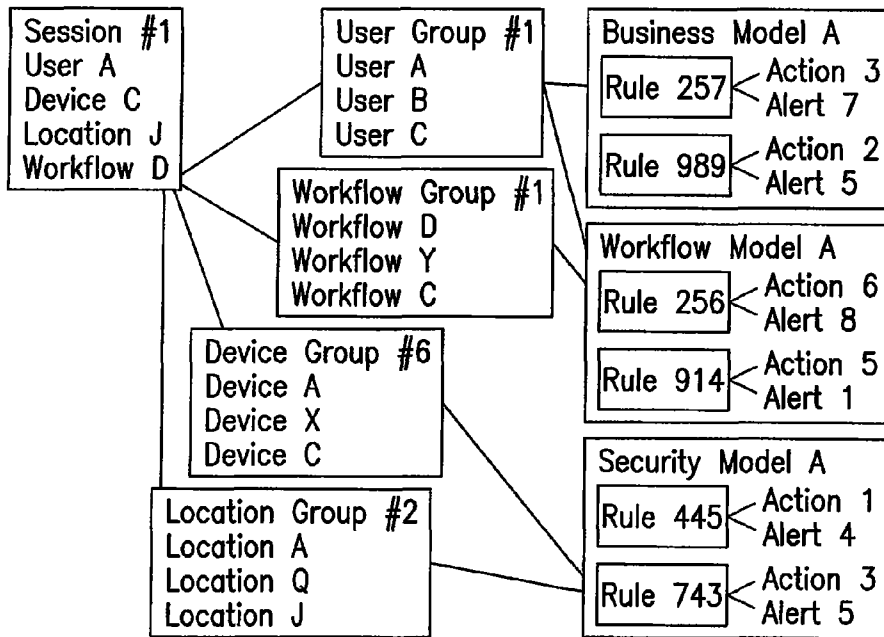


FIG. 16B

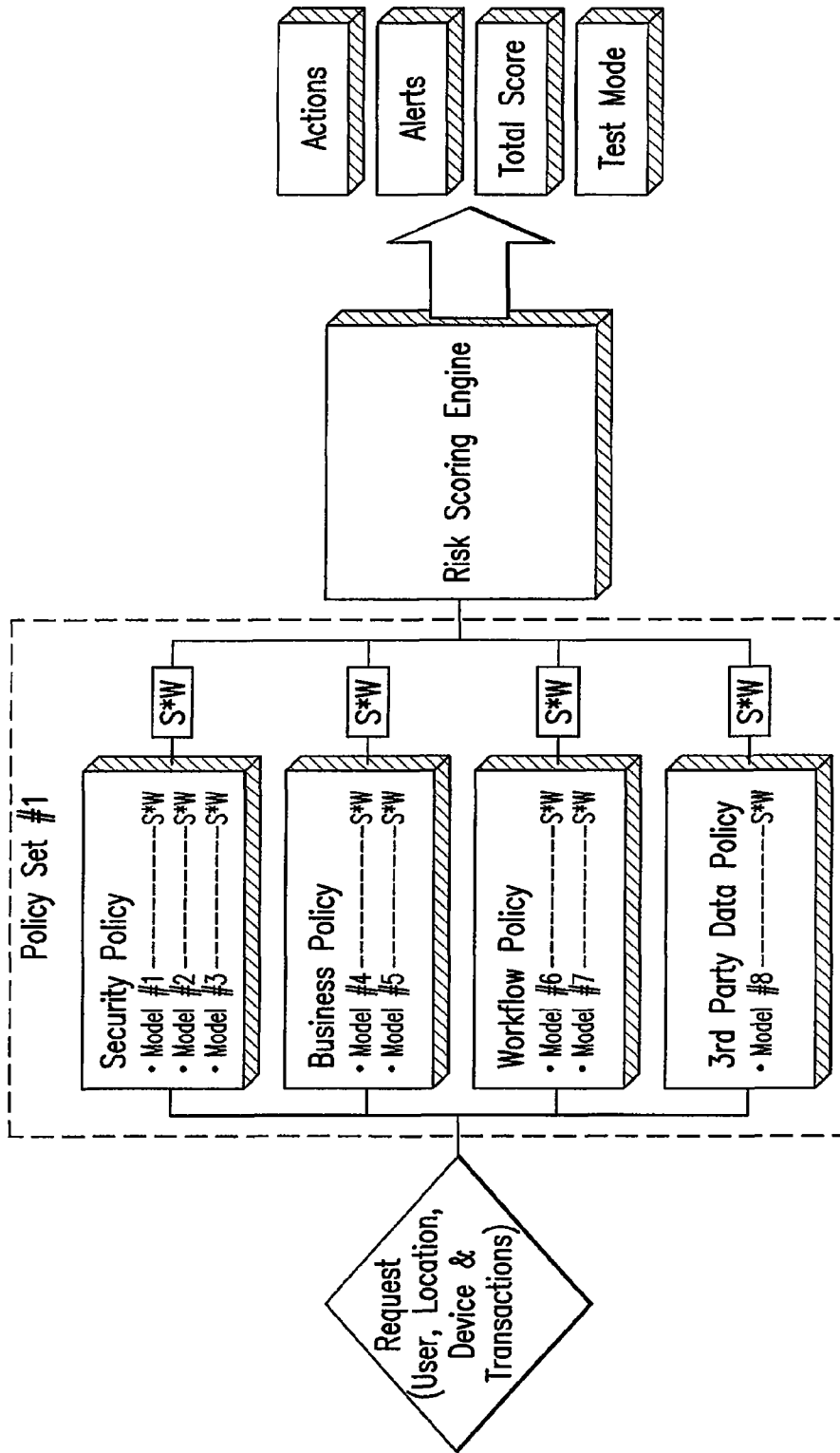


FIG.16C

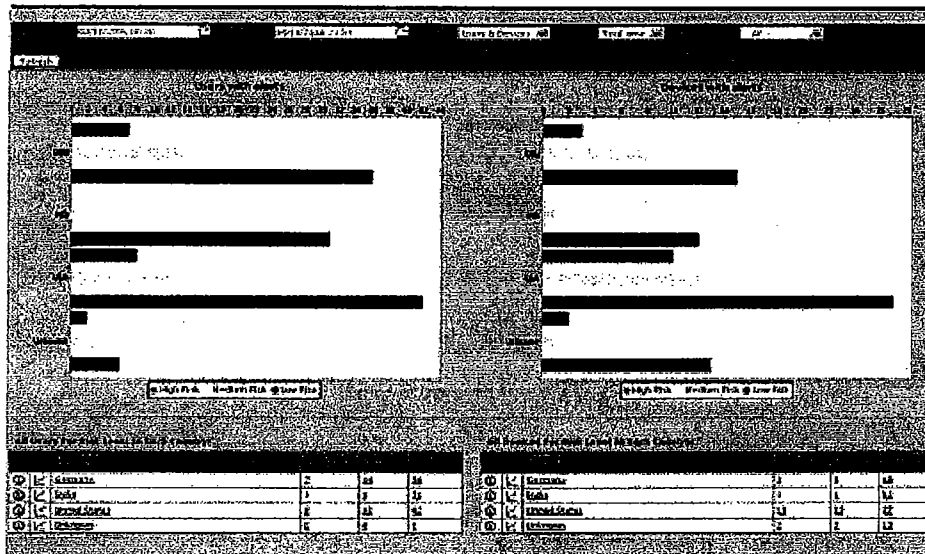


FIG. 17A

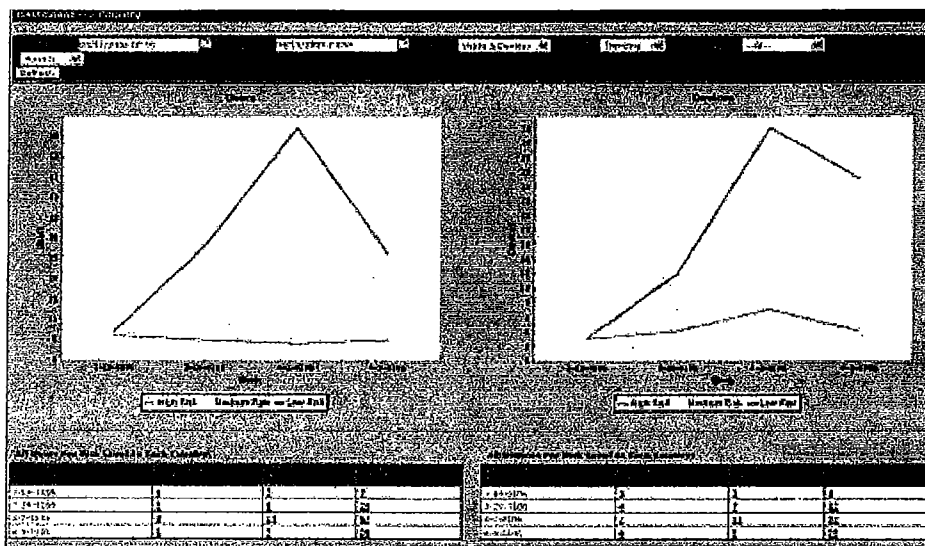


FIG. 17B

The screenshot shows a web application interface. On the left is a sidebar menu with various options. The main area contains a table with several rows and columns. The table headers are partially legible and include terms like 'Item ID', 'Description', 'Quantity', 'Unit Price', and 'Total Price'. The rows contain data for different items, with some cells containing numerical values and others containing text descriptions.

FIG. 17C

The screenshot shows a web application interface for user login. At the top, it says 'Customer Care' and 'Guest Details'. Below this is a login form with a 'Login ID' field containing the value 'jsh200', a 'Password' field, and a 'Remember Me' checkbox. There is also a 'Log In' button. Below the login form, there are links for 'Forgot User Info' and 'Forgot Password', and a 'Sign Up' button.

FIG. 17D

1

SYSTEM AND METHOD FOR FRAUD MONITORING, DETECTION, AND TIERED USER AUTHENTICATION

CROSS REFERENCE TO RELATED APPLICATION

This application claims the benefit of U.S. provisional application Ser. No. 60/676,141 filed Apr. 29, 2005 and which is incorporated herein by reference in its entirety for all purposes.

FIELD OF INVENTION

The invention relates generally to systems and methods for providing protection against identity theft over a computer network.

BACKGROUND OF INVENTION

The growth in the volume of online transactions conducted by businesses and individuals over the Internet has been staggering. Sensitive private identity information is typically used for authenticating a user for conducting online transactions. The increased use of identity information for Internet transactions has been accompanied by an increased danger of interception and theft of that information. Identity theft occurs when someone uses the password, username, Social Security number, credit card number, or other identifying personal information of another without consent to commit fraud. According to a September 2003 Federal Trade Commission (FTC) survey, 27.3 million Americans have been victims of identity theft in the last five years, including 9.9 million people in the year 2002 alone. Identity theft losses to businesses and financial institutions in 2002 totaled nearly \$48 billion and consumer victims reported \$5 billion in out-of-pocket expenses, according to the FTC survey.

To enter into a transaction with an E-commerce server, a user typically needs to provide sensitive and confidential data including authentication data, data describing the transaction, and the like. This data is commonly entered by using a keyboard and/or a mouse connected to a device local to the user that is running a web browser that is linked to the Internet (or other computer network). FIG. 1 is a diagram illustrating an exemplary system 10 used for entering user authentication and transaction data. In this example, the authentication information to be entered by a user comprises a user ID and password. In known systems, the user ID and password are composed of a string of characters entered via a keyboard 12 while executing a web browser on a computing device 14. A typical user entry interface 18 provided by the browser to the user on a display 16 is shown.

After entry, a user's sensitive information is typically transmitted to a remote server preferably in an encrypted form over secure connections. For example, the widely-used TCP/IP communication protocol includes security protocols built on the secure socket layer (SSL) protocol to allow secure data transfer using encrypted data streams. SSL offers encryption, source authentication, and data integrity as a means for protecting information exchanged over insecure, public networks. Accordingly, many E-commerce servers and applications use SSL, or similar security protocols, to exchange data between remote servers and local user systems. If the entered authentication information is approved by the server, the user is permitted to send and receive data from the server's website.

2

The source of messages received at a web server is often determined from the IP address of the device from which the message is sent and/or from a cookie included with data from the user. A cookie generally refers to a packet of information, often sensitive information, sent by a web server to a browser resident on the user's computer system for saving to a file and for transmitting back to the server whenever the user's browser makes additional requests from the server. The IP address is generally included in a message header, and the cookie is usually one that has been previously sent by the server, often at login. The server compares the user login data with the message IP address and the returned cookie to determine the identity of the user sending the message and whether the user is currently logged into the server. The IP address of the user is also confirmed.

Despite these known precautions, a user's sensitive information remains vulnerable because it is in a raw unsecured form between its entry by the user and its encryption prior to remote transmission. Also, sensitive data sent from the server is vulnerable during the period after its decryption and until its display. This unsecured information can be surreptitiously captured in a number of ways. For example, cookie hijackers copy sensitive information from cookies. Further, keyboard loggers and mouse click loggers are hidden software that intercept and copy mouse clicks and depressed keys after user entry but before processing by a browser or other software. Logger software can readily intercept the user's secure information. Keyboard loggers and mouse click loggers might also take the form of hardware connected between the keyboard and mouse cable and the computer or the hardware inside the keyboard and mouse device.

Even graphical user interfaces that represent on-screen keypads and keyboards with selectable graphics for user entry (instead or in addition to providing fields for text entry) are vulnerable to mouse click loggers, screen capture loggers, and other schemes. FIGS. 1, 2, and 3 illustrates prior art examples of such interfaces. Each alphanumeric character in the graphical interface is represented by a unique graphical image, e.g., the pixels forming the number "1". Screen capture loggers utilize optical character recognition (OCR) technology to decipher characters selected by mouse clicks and the corresponding alphanumeric graphics in order to ascertain the actual alphanumeric text characters of a user's ID and password. Sophisticated screen capture loggers might also utilize checksum and size characteristics of the graphic images in order to ascertain which the data item corresponding to a graphic image selected by a user's mouse click during data entry. In these ways, the screen capture loggers may acquire the personal information even when the graphical user interface has rearranged the order of alphanumeric characters on the keypad or keyboard.

Sensitive information can also be intercepted by espionage software, including snoopware, spyware, non-viral malware, hackers utilities, surveillance utilities, Trojan horses, etc. Espionage software aids in the unauthorized acquisition of information about a person or organization without their knowledge or consent. It typically installs itself on a user's computer without consent and then monitors or controls the use of the device. Every user keystroke, all chat conversations, all websites visited, every user interaction with a browser, every application executed, every document printed, all text and images, might be captured by the espionage software. Espionage software typically is capable of locally saving or transmitting the captured data to third parties over the Internet, most often without the user's knowledge or consent.

Another fraudulent acquirer of sensitive personal information is an "over-the-shoulder" spy who surreptitiously reads a user's display to acquire the information.

Known anti-virus and anti-spyware software products attempt to enable a user to protect against such malicious software. However, use of outdated anti-virus and anti-spyware files provides minimal protection, at best, of computer data against outside threats. Consequently, a drawback of these products is that the information used by the anti-virus and anti-spyware program must be constantly updated to reflect newly discovered schemes in order to keep the protection current. In addition to keeping the virus information current, the system must be periodically scanned for potential infections.

Further, certain geographic locations are known to contain an inordinate number of identity thieves. It is therefore advantageous to know where an attempt to access a server originates from. IP addresses are one readily available source of location information. But IP addresses have drawbacks in that, for many users, the IP address is not constant. Known network protocols and facilities can lead to variable IP addresses. For example, proxy servers are used to provide a gateway between a local area network of an organization and the Internet. The local network is protected by firewall software installed on the proxy server. Proxy servers dynamically assign new IP addresses to a user device each time a new message is sent therefrom. As a result, there is no constant IP address assigned to an individual user device for users connected to the Internet via a proxy server.

Another source of IP address variability is the commonly used dynamic host configuration protocol (DHCP protocol) which assigns IP addresses dynamically and automatically to the devices on a TCP/IP network. A DHCP server assigns an IP address to a device from a list of available addresses when the device connects to the network. The device retains this IP address only for the duration of the current session. Some DHCP server systems can dynamically change the user's IP address during the session. The use of a proxy or DHCP server means that the IP address alone may not be enough to identify a particular user device.

Security systems and methods that protect against the above-identified risks should also meet the usability concerns of an average user. A service provider wants to encourage online use in a secure manner. But a cumbersome and prolonged user interface or a less user friendly interface might discourage or even intimidate and frustrate users, or cause user errors, or the like. Also a security system should institute precautions to prevent execution of a fraudulent transaction once it has been found that the user's information and/or system is at risk of being compromised. A security system should also alert the service provider based on a particular device attempting to access the provider's system irrespective of the user.

Also, a security system and method should enable a service provider to strike a proper balance between security and usability of the system. In other words, a system and method is needed to enable a service provider to provide an easy to use and lower security interface when no security risk is identified, and a higher security interface when one is identified. Additionally, desirable security systems and methods should depend as little as possible upon human action to maintain their state of security. For example, it not advantageous to require users to keep and maintain tokens or digital certificates or the like. A token can be lost, damaged, stolen and the like.

But security systems protecting against the described threats and having the described properties are not generally

known in the art. What is needed but currently lacking in the art is a security system and method with the following features and aspects:

- is a device-based fraud monitoring system;
- provides robust fraud monitoring and detection along with robust fraud analysis and risk assessment so that online service providers have real time information needed to determine how and whether to allow a device to access the provider's system;
- provides selectable levels of secure user authentication as a function of usability and/or security concerns;
- ascertains the security risk that a user's information and/or system have been compromised and if so, provides a more secure login interface to guard against fraudulent activity;
- a repository of information for identifying legitimate and fraudulent users based on more reliable and robust fingerprinting of the user device that can be integrated with other repositories of security tracking information;
- is a purely software based solution to identity theft that does not require hardware devices to be issued and maintained;
- is convenient for online users.

SUMMARY OF THE INVENTION

The systems and methods of the present invention fill gaps in the prior art by providing improved authentication services.

An advantage of the systems and methods according to the present invention is that they provide information and selectable user interfaces for enabling a service provider to take action to authorize, deny, or put on hold online transactions in real time as a function of the risk presented by both the user and the device attempting to conduct a transaction.

Another advantage of the present invention is that it enables a service provider to identify possible in-process fraudulent authentication transactions, based on both user and device historical data analysis. Transactions can be approved, declined, or put on hold for verification based on a set of predetermined rules.

Another advantage of the present invention is that it provides both user and device based robust fraud monitoring and detection along with robust fraud analysis and risk assessment to give a service provider real time information needed to determine how and whether to allow a device to access the provider's system.

Another advantage of the present invention is the enabling of a selection of levels of secure user graphical authentication as a function of predetermined usability and/or security concerns.

Another advantage of the present invention is that there is no dependence on tokens, cards and other similar hardware devices, digital certificates, anti-virus software, or personal firewall solutions for protecting end users against online identity theft.

Another advantage of the present invention is the acquisition and development of a blacklist and/or white list that is device based rather than only user based.

Broadly stated, according to an embodiment, the present invention fingerprints a user's device by obtaining device identifying information that can be used to assess the fraud risk posed by a user at that user device. According to another embodiment, the present invention performs fraud analysis and alerting of the risk associated with the device being used to access a service provider's server. According to another embodiment, this invention includes a database of user

5

devices and their historical known fraud risks available in a central repository. According to another embodiment, this invention presents user authentication interfaces selected from a plurality of user authentication interfaces that provide a plurality of levels of security and usability.

Accordingly, the present invention provides systems and methods for providing levels of fraud monitoring, detection, and a tiered user authentication comprising a fingerprinting module for identifying a user device that has requested connection to a server; an authenticator module for enabling selection from of a plurality of login graphical user interfaces as a function of predetermined selection criteria for presentation on the user device, wherein the selection criteria is in the form of rules regarding usability and security; a fraud analyzer and alert module for analyzing and assessing the risk associated with the user device as a function of historical tracking of use of the user device; and a device central repository for identifying legitimate and fraudulent users based on the fingerprinting module and other repositories of tracking information. This invention provides variously architected systems that implement the methods of this invention to provide authentication services to one or more service providers.

An example of the present invention's usability and security features is provided by users who have forgotten their login id or password. Such a user typically accesses a system from a limited number of user devices, and the fact that authentication attempts of this type were made from such a device is recognized by the present invention and can be used to present a helpful interface to the user. If the device is unknown to the system, this can signal that a hacker is trying to break into the system and can be used to present an authentication interface of heightened security. Additionally, such users typically enter his user/password information that is almost but not entirely accurate. This can be recognized by the present invention and used to further guide user authentication. In preferred embodiments, these options are represented by rules processed by a rules engine.

A further example of this invention's usability and security features is provided by the ability to distinguish user behaviors. If an access originates from a user device that has not previously accessed a service provider (e.g., as detected by the absence of a device token stored on the user device), system rules can require that this access pass a higher level of authentication or challenge. However, the user may be a savvy user who routinely removes application tokens from their user device (almost 15% of Internet users). Further, on the basis of previous accesses, this user may be associated with a behavior pattern indicating routine access from not-readily-identifiable devices. Then, this user is preferably not challenged or subject to a higher level of scrutiny. In contrast, systems with authentication systems that do not adjust the authentication process on the basis past user behavior would always challenge such a user. Accordingly, the present invention provides a better user experience for all the users, whether they are savvy or not.

In further detail, the systems and methods of the present invention verify each user's computer and location ("something you have") along with behavioral usage patterns on a site to confirm identity ("something you are"). These verifications are added on top of existing enterprise requirements for login/password credentials ("something you know"). This offers the enterprise several strong additional layers of anti-fraud protection.

The present invention includes secure cookies, flash objects and other technologies to recognize and to fingerprint the from which device a user access an application, whether it is a computer, laptop, mobile device or any other. These user

6

devices thus become additional authentication factors without requiring any change in user behavior. Information concerning these user devices is fingerprinted and stored into a device token or device id for one-time use. The id or token is stored on the user device and saved in a database for later comparison with tokens retrieved from subsequent user device accesses. The token is invalidated if a user attempts to reuse it.

The present invention also includes user device tokens or device ids that have a unique number which is randomly generated by the methods of this invention. Such device tokens are then assigned to the particular user device, stored on the particular user device as persistent data (e.g., a cookie), and also stored so as to be accessible to the authentication services of this invention. The particular user device can be thereby identified upon a subsequent access by retrieving the device token from the user device and comparing the unique number with the stored information. If the data matches, this particular device is identified. Then a new unique identifier number is created and is stored on the user device and by the methods of this invention for use in a further access.

The present invention enables application service providers score risk for each online login and transaction and to increase authentication security in real time, at login and in session, for transactions that may be high risk or potential fraud. It evaluates the pre, post and in-session characteristics of each transaction to ensure fraud detection and transactional integrity. The methods then provide a service provider with scores, actions, and alerts. For example, if a transaction has a high risk score and is thus potentially fraudulent, one preferred action is to hold the transaction and to then seek secondary authentication or secondary challenge. The user is, e.g., asked to call service provider personnel to confirm the validity of the held transaction. Another action is to reject the transaction. Different actions may be appropriate to different transaction types. In the case of banking service providers, viewing account balances is acceptable but wire transfers are not acceptable; or in the case of ecommerce/ASP service providers, download of sensitive documents may be restricted based on the risk score. These actions are preferably invoked by rules evaluated during transaction evaluation.

The systems and methods of the present invention include the following features: device, location and user behavior ("workflow") fingerprinting; user profiling through capture and recording of user workflows; real-time risk scoring; real-time, rules-based fraud alerts and response; alerts; automatic internal flagging of suspicious activity; configurable, out-of-band end-user optional secondary authentication (via e-mail, SMS, voice print other); 3rd party integration via open APIs; support for shared authentication and fraud services infrastructure; case management tools for reviewing individual client logs; customer care tool for servicing inbound customer care; a dashboard for real time fraud and activity monitoring; reporting for risk management and trending analysis; and administration for system and rules configuration and maintenance. The methods and systems include the following components and features: rules engine; risk scoring/forensics; real-time response; proprietary fingerprinting of devices, locations, workflows; models and rules; intelligent algorithms; and comprehensive administrative tools such as a dashboard, reports, and customer care

These and other embodiments, features, aspects, and advantages of the invention will become better understood with regard to the following description, appended claims and accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

The foregoing aspects and the attendant advantages of the present invention will become more readily appreciated by

reference to the following detailed description, when taken in conjunction with the accompanying drawings, wherein:

FIG. 1 is a diagram illustrating an exemplary prior art system used for entering user authentication;

FIG. 2 illustrates a prior art keypad graphical user interface for enabling entry of authentication information via mouse click selections;

FIG. 3 illustrates a prior art keyboard graphical user interface for enabling entry of authentication information via mouse click selections;

FIGS. 4A-B illustrate flowcharts depicting an exemplary embodiment of the fingerprinting aspect of the system and method of the present invention;

FIG. 5 illustrates a flowchart depicting a process illustrating an exemplary embodiment of the system and method of the present invention;

FIG. 6 illustrates a Fraud Analyzer and Alert System (FAAS) aspect according to an embodiment of the present invention;

FIG. 7 illustrates a block diagram of an authenticator for enabling selection of one of a plurality of login graphical user interfaces as a function of a selection criteria, according to an embodiment of the present invention;

FIG. 8 illustrates a graphical wheel two-factor authentication interface for enabling authentication information entry using mouse click navigation for aligning alphanumeric and graphic symbols according to an embodiment of the present invention;

FIG. 9 illustrates an exemplary graphical slider authentication interface for enabling authentication information entry using mouse click navigation for aligning alphanumeric and graphic symbols according to an embodiment of the present invention;

FIG. 10A illustrates a selectable higher security keypad graphical authentication interface for providing higher security including the reordering of the alphanumeric symbols in the interface in FIG. 2 according to an embodiment of the present invention;

FIG. 10B illustrates a selectable higher security keypad graphical authentication interface for providing higher security including offsetting the keypad in the interface in FIG. 2 in one direction according to an embodiment of the present invention;

FIG. 10C illustrates a selectable higher security keypad graphical authentication interface for providing higher security including offsetting the keypad in the interface in FIG. 2 in another direction according to an embodiment of the present invention;

FIG. 10D illustrates a selectable security keypad graphical authentication interface for providing higher security including distortion of the alphanumeric keypad entry choices in the interface in FIG. 2 according to an embodiment of the present invention;

FIG. 10E illustrates a selectable higher security keypad graphical authentication interface for providing higher security including reordering along with shading of a portion of the interface in FIG. 2 according to an embodiment of the present invention;

FIG. 11 is flowchart illustrating an exemplary device central repository (DCR) system and method according to an embodiment of the present invention; and

FIG. 12 is a block diagram illustrating an embodiment of the flagged devices module (FDM) of FIG. 11;

FIGS. 13A and 13C illustrate exemplary system implementations of the present invention;

FIG. 13B illustrates an exemplary method structure implementation of the present invention;

FIG. 14 illustrates a preferred function configuration of the present invention;

FIGS. 15A-B illustrate an exemplary policy set and an exemplary security model for inclusion within the exemplary policy set;

FIGS. 16A-C illustrate a preferred structure for the external objects and models of the present invention; and

FIGS. 17A-D illustrate exemplary administrative tools.

Reference symbols or names are used in the Figures to indicate certain components, aspects or features shown therein, with reference symbols common to more than one Figure indicating like components, aspects or features shown therein.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

This invention generally provides systems and methods that interface with service providing systems of online service providers and assists them in authenticating their user requests, especially user log on requests and transaction sequences (referred to herein as a user's "workflow"). Briefly, this invention authenticates a user and a login request (referred to herein as "pre-authentication") in a manner determined both by the identity of the device from which the authentication request originates this invention as well as by available information concerning the identity of the requesting user. User workflow sequences are authenticated (referred to herein as "post-authentication") using a user's transaction history. In both applications, the precise authentication processes and decisions can be directed by rules from the service provider.

Preferred System Configurations

The general structure and arrangement of preferred embodiments of these systems and methods are now described, following are more detailed descriptions of preferred embodiments of the component processes. Heading are used herein solely to aid clarity and without any intended limitation.

FIG. 13A illustrates an exemplary embodiment of the present invention directed to providing authentication services to online service providers who make available to individual users online server applications. Generally, the server applications execute on service-provider server machines. The embodiment illustrated includes one or more service-provider computer systems, e.g., systems 1302 and 1304 and an authentication system server system 1306, interconnected through network 710 to one or more user devices 720 at which users enter logon and subsequent transaction requests. The systems server 1306 is generally structured as known in the art, and includes a CPU, RAM memory, disc or other database memory 1308, communication interfaces, optional user interface equipment, and the like. Databases 1308 for store data used in authentication processes, such as device and user histories. The network can also be generally structured as known in the art and can be a private intranet, the public Internet, or the like. The user device from which a user makes requests to server applications can be a workstation-type computer, a PC-type computer, a terminal, if the like.

In many preferred embodiments (but without limitation), the authentication processes of the invention are implemented with a client-server-type architecture (or, more generally, a distributed-systems-type architecture). Accordingly, the individual processes providing authentication services for a particular service provider application can both execute on the service provider's computer system or be distributed among other network-attached computer systems. Preferred distri-

bution architectures include one or more authentication servers that at least host a device central repository (“DCR”) service.

The DCR receives, stores, and makes available online information 1310 identifying user devices and the fraud risks associated with the user devices. This information can include blacklists and/or white-lists of devices with higher risk of fraud and with lower risk of fraud, respectively. This information can be gathered from the authentication experiences of the service providers participating in an implementation of this invention, or from other concurrent and inter-communicating implementations of this invention, from 3rd party data sources, and the like. Authentication servers can also host service provider applications.

Optionally, the authentication server can also host the actual authentication processes of this invention, which are then configured as server processes responding to requests from application executing remotely on service provider computer systems. Thereby in certain embodiments of this invention, the authentication server system also provides “device-based authentication services” as well as “DCR services”. A service provider server system, e.g., system 1304, for example, need itself not run all (or any) authentication processes, but instead can access those processes it does not host (or all authentication processes) on the authentication server. In other embodiments, a service provider system can execute all authentication processes, and therefore need only access the authentication server for optional DCR services. In FIG. 13A, system 1302 does not itself perform pre-authentication processing, but does performs “post-authentication services”.

authentication protocols, such as a security question, before allowing access. This embodiment is applicable to an entity such as an organization, company or law firm for authenticating remote log-ins from its employees, members or other users, where these employees or users number approximately 10,000 or less.

FIG. 13B illustrates the computer-implemented processes that cooperate to provide the authentication services, primarily pre-authentication services, of this invention. In the illustrated preferred embodiment, these processes are structured as shown within the enclosing dotted lines and include: fingerprint processes 400, fraud analysis and alert service (“FAAS”), authenticator service 600, and flagged device module (“FDM”). Links between processes are labeled by important input and output data types.

Authentication services are invoked when a server application or services provider computer system receives user request 1320 that needs authentication. In the case of pre-authentication, the most common user request is a login request to access an application or system. Other requests usually handled by post-authentication services include, e.g., transaction requests involving large amounts of money. User requests can be received directly from communication subsystems, or alternatively, can be forwarded from the service provider application or system across an interface to the authentication processes.

In preferred embodiments, authentication services can be invoked through an externally available application programming interface (“API”). Table 1 list a selection of exemplary API requests.

TABLE 1

Example API requests				
#	Description	Action	Request XML	Response XML
1	Pre-authentication request to fingerprint the device	FingerPrintRequest	FingerPrintRequest.xml	FingerPrintResponse.xml
2	Updates the authentication status for the authentication session	UpdateAuthResult	UpdateAuthResultRequest.xml	FingerPrintResponse.xml
3	Processes the rules	ProcessRules	ProcessRulesRequest.	ProcessRulesRespon

In another preferred embodiment, authentication services, usually pre-authentication services can be performed on a firewall machine (or other type of network gateway machine). In FIG. 13A, firewall 1305 performs primarily pre-authentication services for service-provider system 1304. If a user is authenticated, then that user can access service provider applications, e.g., applications A, B, C, D, and so forth. In certain instances, a firewall can perform all pre-authentication service processing; however, in most instances, it is advantageous for the firewall to act as a client to the authentication services of the authentication server. In fact, it may not be practical for a firewall to perform full pre-authentication processing even with server assistance, in which case it can perform a subset of authentication processing (referred to herein a “basic authentication services”).

Basic authentication services can be limited to user device fingerprinting and confirmation of basic machine data, e.g., IP address, operating systems, device ID, and the like. As described subsequently, the user’s computer is provided with a cookie that includes the identifying information of the machine. This cookie is reviewed by the firewall upon login to verify that it matches what the entity knows about the user. Discrepancies can be identified and scored to determine whether to allow access or not or whether to apply secondary

The first request would typically be sent from a service provider application to begin an authentication of a device from which a user request has been received. The second request can be sent when the service provider application wishes to check authentication status for performing, e.g., a high-value transaction. Finally, the third exemplary request can provide rules and have them processed in view of the current authentication information characterizing a user or session.

Fingerprint process 400 is the first authentication process invoked with input data describing the user request. The fingerprint process then gathers identifying information describing the device from which the user request originated and creates a device identifier (“Device ID”). The Device ID (and optionally other device identifying information) is stored on the user device from which it can be retrieved and form part of the device identifying information to be used during a subsequent fingerprinting

Next, FAAS process 600 is invoked with the Device ID (and optionally other device and/or user identifying information). This process evaluates its input identifying information and either can, e.g., recommend to the service-provider application or system that the request should be processed further or blocked from the system (referred to herein as “actions”). This process can also provide risk alerts and risk scores (re-

ferred to herein as “alerts” and “scores”) describing the relative risks of the input request so that the service-provider application or system can themselves make such authentication decisions. FAAS evaluation preferably begins with retrieving forensic information related to the characteristics of the current request that are apparent in the input request information. Information sources can include system DCR services, which stores an authentication system’s past authentication results, and third party data services, which can provide a wide range of data, e.g., geolocation data services providing likely geographical source of the current request. The input data and the retrieved forensic data is then analyzed by a rules-based decision process in order to determine output actions, alerts, and scores.

In other words, device id is usually available and then is the primary item to identify an authorized user. Even when the device id is recognized, the user can be required to provide additional security information before being allowed access. Other conventional security protocols (i.e., personal questions, selection of personal information from a multiple choice question, etc.) or even a higher level of security (i.e., telephone IP administrator, call to provide voice recognition, etc.) can be used. When a user knows in advance that a different computer will be used for access at certain times, e.g. business travel to a new location with use of a different computer contemplated, then this information can be provided to the entity and its IP administrator so that the rules for that particular user and time period can be changed to facilitate access to the system and its application.

If a request is to be further processed, a further exemplary action is the selection of preferred graphical (or other type) authentication interfaces (“GUI”) for authenticating a newly arrived user or an existing user making a request that needs particular authentication. Authentication interface selection criteria can be determined in accordance with the evaluated risk scores and any risk alerts. The selection criteria will then call for an interface with a security that is commensurate the risk of fraud. Also, the risk information can also be provided to the service provider system or application which can then perform, e.g., more thorough checking of authentication data or requesting the authentication services of this invention to re-authenticate the user or request. This can involve, e.g., seeking responses to details authentication questions, or obtaining biometric identification information (e.g., fingerprints, retinal scans, or the like), or obtaining voice prints, or the like.

Next, authenticator process 700 is invoked with the interface selection criteria, selects a particular user authentication interface from a user-interface database according to the criteria, and then presents the selected interface at the originating user device, and receives the data entered in response to interface presentation. The entered data is then used as part of the authentication decision by the service provider application 1322 of processes of this invention. The server application, or the FAAS, or both together then decide whether on not to authenticate the current request.

The DCR process gathers the results of the current request-authentication processing and stores them in DCR database 1110 in association with the identifying information (for example, the Device ID) for the originating user device. These stored processing results preferably include, at least, whether or not the request was validated or not and/or whether or not the request was found to be fraudulent. Thereby, the DCR database can provide an historical record of the results of previous request-authentication processing to guide the FAAS in current authentication-request processing. The DCR database includes at least data obtained from the

current service provider. Preferably, it also includes data from other service providers so that device risk information can be shared and the accuracy of authentication processing can be multiplied.

FDM 1200 performs the actual gathering and assembly of the results of the current request-authentication processing. Data from the current request can optionally be supplemented by the third party data similar to that data already retrieved by the FAAS and/or other data retrieved by the FAAS relevant to evaluating the current request. The FDM process can execute either locally or remotely as part of authentication services, or can be implemented as part of DCR services.

FIG. 13C illustrates computer-implemented processes for an exemplary embodiment of the basic authentication services that might be invoked (locally or remotely) by a firewall or router. This particular embodiment performs only the minimal processing necessary to authenticate according to this invention, rules engine process 701. This process is invoked when a user request is received by, e.g., a firewall, and receives information describing the request. In one alternative, this process determines actions and scores from input data descriptive of the user transaction and rules retrieved from database 1809 (either supplied by a service provider or default rules available from the authentication system). The rules can be either proactive or reactive. For example, access can be blocked unless the fraud risk is low, or allowed unless the fraud risk is high. In other alternatives, process 701 can also retrieve and rely on data from the DCR database and/or 3rd party sources. Actions, scores, and/or alerts are then provided for further processing by the firewall 1322.

In other words, when the system finds an elevated risk score, it evaluates rules in view of the risk score and can carry out actions, alerts, or risk score reporting. Table 2 provides preferred categories of responses to an elevated risk score.

TABLE 2

Events & Risk Scoring Engine
Determine and output weighted risk score
Customizable thresholds
Customizable actions
Customizable alerts

An exemplary action is the setting of an Internal flag or adding to a watch list so that the service provider can follow up later. Another exemplary action is online or out of band secondary authentication, preferably based on a challenge response model. For example, online secondary authentication can require a user to response to an email sent to a registered email address. Out of band authentication can include various biometrics such as a voiceprint which can require a user to verbally a response to a challenge.

The methods of this invention retrieve information concerning a device from which a request originates, the user originating the request, and the transactions requested by that user. Efficient handling of this information is advantageous, especially in commercial applications servicing a large number of concurrent users. Thus in many preferred embodiments gathered information is stored for online use in a condensed or summary form, and for offline use in nearly full or full detail. Online uses include, e.g., real time authentication and authentication update. Offline uses include, e.g., data mining, rule refinement, and so forth.

A preferred condensed or summary form is referred to herein as a fingerprint. First, possible values of a category of data or of an authentication criteria are divided into a number of “bins”. Then the category or criteria fingerprint of a par-

particular user is a representation (e.g., as a binary token) of the gathered data which indicates only which bins have data and which do not. This representation can be optionally compressed using known techniques. Thereby, a user's authentication and transaction requests can be represented in several binary tokens.

For example, in a typical online business application, there may be 20 unique pre-identified sensitive transaction sequences (workflows). Each workflow can be characterized by, e.g., ten bins or variable with each variable having, e.g., ten bind of values. Therefore, a user can be characterized by a fixed number of possible fingerprints with each user having on average, e.g., ten unique fingerprints.

Preferred Functional Configurations

The function of the present invention are configured to provide consistent methods of checking the authenticity and security of a user-initiated request made to a service-provider application, e.g., a online store application, an online banking application, and the like. The methods receive a copy of the request itself or information describing and abstracting the substance of a current request. The input information is processed, and the methods output risk scores, risk alerts, and actions (or action recommendations). Risk scores and alerts are indicia of the likely risks that the current request is incorrect, or malicious, or fraudulent, and so forth. More specifically, the risk scores output are products of a number fraud detection inputs which are weighted and analyzed in real time using analytic processes customizable for individual service providers. Fraud detection inputs describe the user, the user's device, the location of the user's device, the workflow of transaction entered by the user, historical patterns of user accesses, and data from 3rd party data sources. This information is provided to service-provider applications and systems ("users" of the invention) for use in their internal authentication processes. The methods of this invention can also recommend or initiate actions according to service-provider guidelines or rules. These actions are generally directed to gathering information for authenticating the request being processed.

Generally, the available, security-relevant information related to a user request (the "request attributes") is broken into related information groupings referred to as criteria so that each criteria preferably contains several pieces of data concerning a user request. Groups of rules, preferably criteria-specific, then evaluate the criteria, and the risk scores and actions that are output result from a combination and weighting of the results of the rule-based evaluation of each criteria. As a user request, and especially as a related group of user transactions, is authenticated by this invention and processed by service-provider applications, more or less criteria data are available and criteria have varying importance. For example, before a user is authenticated and granted access to a service-provider application, data relevant to workflow criteria (e.g., a sequence of related transactions by a user) is usually not available. On the other hand, when a user is engaged in requesting transactions, criteria related to initial authentication are usually less important. These periods are referred to as the "pre-authentication" period and the "post-authentication" period respectively.

Preferred pre-authentication criteria include location information and device information, and preferred post-authentication criteria include user information and workflow information. Table 2 present exemplary data relevant to each of these criteria.

TABLE 3

Example of Request Attributes			
5	Pre-authentication	Location information	City, State, Country information and confidence factors Connection type Connection speed IP address, routing type, and hop times Internet service provider flag Autonomous system number Carrier name Top-level domain Second-level domain Registering organization A list of anonymizing proxies Hostnames and routers
10		Device information	Secure Cookies Flash Cookies Digitally signed device Device & display Characteristics: Operating System characteristics Browser Characteristics
15		User information	User identifications Valid or not valid user Authentication status
20	Post-authentication	Transaction information	Key Value Pairs: Support multiples Keys can be defined using Regular Expressions Values can be defined in ranges Pages accessed Time spent on page Transactions sequences

FIG. 14 illustrates an exemplary functional configuration including the request attributes and criteria of Table 2. The request attributes of the criteria are condensed into fingerprints: a location fingerprint, a device fingerprint, a workflow fingerprint, and an historical data fingerprint. The fingerprints are then processed to generate actions, alerts, and scores. Possible actions include primary authentication, which is the process by which the user is identified and authenticated. Primary authentication based primarily on location and device fingerprints and can include presentation of secure logon screens at the user device. Another action is secondary authentication, which can be invoked during a session if authentication confirmation or further authentication is needed. It can include use of, e.g., email, voiceprints, and the like.

This figure also illustrates that 3rd party data can be included in the evaluation process. Third party data can be incorporated in various fingerprints. For example, third party data can include the presence or absence of firewall or of antivirus software on a user device, and also and/or the maintenance status of such software. Third party data can also include IP Intelligence, risk data, historical data (from a data warehouse), fraud network data, and so forth. Further, third party describing characteristics of known risks at the location, device, or user level can be received from third party data warehouses and incorporating in various fingerprints, primarily the workflow fingerprint and the historical data fingerprint. Also 3rd party evaluation tools can integrated into or supplement the analytics and scoring process the evaluates the fingerprints.

Location information and device information are important criteria, especially in the pre-authentication period. Location information characterizes the location of the device from which a request originates. Location can most easily be estimated from the device's IP address and the hierarchy of networks linking the device to the Internet. Device information characterizes the originating device itself, such as its hardware and software components. Table 3 present a more

15

detailed catalog of device software and hardware characteristics that can be extracted from a device by a browser-hosted process.

TABLE 4

Exemplary hardware and software characteristics			
Device Information		HTTP Header	Flash Shared Object
Operating System	Operating System	X	X
	Version	X	
	Patch	X	
Browser	Browser	X	
	Version	X	
	Patch level	X	
	Http protocol version	X	
Hardware	Screen DPI		X
	Has Microphone		X
	Has Printer Support		X
	Has Audio Card		X
	Screen Resolution		X
	Screen Color		X
Software	Has Audio Encoder		X
	Supports Video		X
	Has MP3 Encoder		X
	Can Play Streaming Audio		X
	Can Play Streaming Video		X
	Has Video Encoder		X
	Location		
	Location	X	
	Language	X	X
	Language Variant	X	

A further important component of device information when available is a secure token, e.g., a secure cookie, available from a device which has been previously used as a user device. When a request is received from and device, at least the available location and device information can be summarized, condensed, or fingerprinted and stored back on the device as a secure token. If another request then originates from this device, the secure token can be retrieved and its contents compared against the currently-collected location and device information. Any mismatches can be weighted to form a score for use in risk analysis. Whether or not mismatches occur, a new secure token is generated from the currently-retrieved information and stored back on the device.

Such a secure token also advantageously includes a unique identifier generated by the methods of this invention. Comparing the unique identifier in a retrieved token with an expected or known unique identifier provides further information on which to base the score. Also, a unique identifier is particularly useful if location or device information cannot be obtained from a user device. Then the unique token can be the only identifying device information.

Preferred post-authentication information includes user information and transaction (or workflow) information. User information includes user identification and the progress of a user through the user authentication process. Transaction information includes information extracted from a requested transaction and the sequence and timing of transactions. Information is preferably extracted from a transaction request by looking for key expressions and then extracting the values (perhaps only ranges of values) and other information associated with the key. Sequence and timing of transactions and of web pages visited is packaged into workflow fingerprints which are summaries of a users historical usage patterns.

FIG. 14 also indicates that the criteria data, packaged into fingerprints as already described, is processed and scored in real-time by fraud analytics driven by a rules engine. In order

16

to provide authentication services concurrently to multiple service providers and service provider applications, the analytics and the rules defining this processing are preferably grouped into functionally related modules that are seen as substantially interchangeable by the rules engine. Thus authentication services can be provider to various service providers by having a generic rules engine (or a few instances of a generic rules engine) switch between modules. Each service provider can define its own authentication services by providing or more of this modules.

Analytics are thus preferably implemented in groups what are known herein as policies. Table 5 illustrates preferred policies that are useful for most systems. Other systems can have some or different policies as needed.

TABLE 5

Policies	
Security policies	Anomaly detection
	Misuse detection
	Intrusion detection
	Predefined hacker models
Business policies	Customizable models
	In session transaction monitoring
	Business defined transaction rules
	Key Value driven logic
Workflow policies	Customizable models
	Event, time and value pattern recognition
	Historical transactions
	Behavioral analysis
	Temporal analysis
	Auto classification
Profiles of users	
Predefined customizable risk models	

Policies can be enforced during pre-authentication, for example when a user is being authenticated, or during post-authentication, for example when a user is making transaction requests. The rules engine automatically determines what models to run based on the context of the request. Different sets of models can be configured to support different transaction types, e.g. bill pay, money transfer, password change, email change, etc. Since the models are defined and written in XML, after the initial integration, no code changes are needed in the service provider applications. All models can be modified using a network interface or by replacing the XML definition file. Also, new models can be added seamlessly during operation of the methods of this invention. Models are fully portable, so that they can be migrated from a simulation environment to a test and production environment. Additionally, policies can be configured for exceptions, like "user not in user list" or "device not a bank kiosk", etc.; policies can be temporarily overridden based on, e.g., time period or one time exceptions.

Briefly, security policies are applicable both pre- and post-authentication and typically seek to recognized known hacker behaviors. These behaviors can be recognized using standards developed from cross-industry best practices. Business policies are primarily applicable post-authentication when a transaction session is ongoing. These policies generally represent standards established by a particular service provider for mitigating transaction risk. Workflow policies are primarily applicable post-authentication and compare fingerprints of past transaction session activities with fingerprints of the current session in order to detect unexpected patterns that may indicate fraud.

FIG. 15A illustrates functional configurations that implement policies, such as the policies of Table 4. Each incoming request is analyzed (preferably concurrently) according to the

