(12) STANDARD PATENT (11) Application No. **AU 2007215180 B2**
(19) AUSTRALIAN PATENT OFFICE

(54) Title
System and method for network-based fraud and authentication services

(51) International Patent Classification(s)
G06F 17/00 (2006.01)

(21) Application No: **2007215180** (22) Date of Filing: **2007.02.12**

(87) WIPO No: **WO07/095242**

(30) Priority Data

(31) Number	(32) Date	(33) Country
60/771,861	**2006.02.10**	**US**

(43) Publication Date: **2007.08.23**
(44) Accepted Journal Date: **2011.03.17**

(71) Applicant(s)
VeriSign, Inc.

(72) Inventor(s)
Siddharth, Bajaj;Adler, Joseph;Lin, Yueqin;Mutu, Alin M.;Ong, Bruce;Burstein, Jeffrey;M'raihi, David;Popp, Nicolas;Loftus, Kerry E.

(74) Agent / Attorney
Shelston IP, Level 21 60 Margaret Street, Sydney, NSW, 2000

(56) Related Art
US 2005/0278192

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
23 August 2007 (23.08.2007)

PCT

(10) International Publication Number
WO 2007/095242 A3

(51) International Patent Classification:
G06F 17/00 (2006.01)

(21) International Application Number:
PCT/US2007/003822

(22) International Filing Date:
12 February 2007 (12.02.2007)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/771,861 10 February 2006 (10.02.2006) US

(71) Applicant *(for all designated States except US)*: **VERISIGN, INC.** [US/US]; 487 East Middlefield Road, Mountain View, CA 94043 (US).

(72) Inventors; and

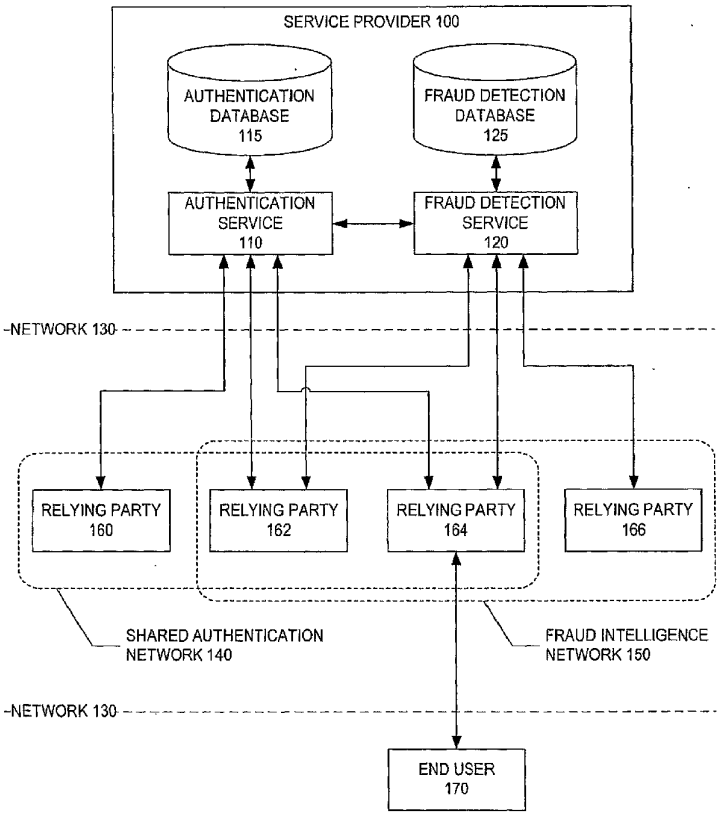
(75) Inventors/Applicants *(for US only)*: **M'RAIHI, David** [FR/US]; 762 Cedar Street, San Carlos, CA 94070 (US). **ADLER, Joseph** [US/US]; 2400 W El Camino Real, Apt. 714, Mountain View, CA 94040 (US). **SIDDHARTH, Bajaj** [IN/US]; 300 Hill Street, #4, San Francisco, CA 94114 (US). **POPP, Nicolas** [US/US]; 196 Santa Monica Ave., Menlo Park, CA 94025 (US). **LOFTUS, Kerry, E.** [US/US]; 2007 Churton Avenue, Los Altos, CA 94024 (US). **ONG, Bruce** [US/US]; 1451 17th Avenue, San Francisco, CA 94122 (US). **MUTU, Alin, M.** [US/US]; 37810 Rose Tree Court, Fremont, CA 94536 (US). **BURSTEIN, Jeffrey** [US/US]; 4538 Tampico Way, San Jose, CA 95118 (US). **LIN, Yueqin** [CN/US]; 5018 Lassen Avenue, San Jose, CA 95129 (US).

(74) Agents: **MORRIS, Gary, S.** et al.; TOWNSEND AND TOWNSEND AND CREW LLP, Two Embarcadero Center, 8th Floor, San Francisco, CA 941 11 -3834 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS,

[Continued on next page]

(54) Title: SYSTEM AND METHOD FOR NETWORK-BASED FRAUD AND AUTHENTICATION SERVICES



(57) Abstract: A system and method for providing identity protection services. According to an embodiment, a validation server receives over a network a response from a credential associated with a user, the credential response provided by the user in order to authenticate the user to one of a plurality of sites on the network that accepts the credential as a factor for authentication, the validation server verifies the credential response on behalf of the one network site, a fraud detection server receives over the network information in connection with a transaction associated with the user at the one network site, and the fraud detection server evaluates the transaction information for suspicious activity based at least in part on information provided to the fraud detection server in connection with one or more transactions at one or more sites on the network other than the one network site.

WO 2007/095242 A3

RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

(88) Date of publication of the international search report:
28 February 2008

SYSTEM AND METHOD FOR NETWORK-BASED FRAUD AND AUTHENTICATION SERVICES

Cross Reference To Related Applications

[0001] This application claims the benefit of U.S. Provisional Application No. 60/771,861, filed February 10, 2006, which is hereby incorporated by reference in its entirety.

Background of the Invention

[0001a] Any discussion of the prior art throughout the specification should in no way be considered as an admission that such prior art is widely known or forms part of common general knowledge in the field.

[0002] Identity theft has continued to grow, and the extent of the problem is significant. Each year, millions of adults in the U.S. have their identities stolen and tens of millions of accounts are compromised, leading to losses from identity theft in the billions. While the fraud losses themselves are significant, even more worrisome has been the negative impact to enterprises whose consumers have been victim to these breaches. Account churn, lower transaction volume and even lower stock prices have made the extent of the losses harder to bear for most enterprises.

[0003] Given the impact of identity theft on online businesses and the regulatory guidance around strengthening authentication, more and more enterprises are evaluating authentication options for their online consumer base. Weak authentication has led to Internet identity theft, phishing, and on-line financial fraud. As more consumers use computers and mobile devices for shopping, managing their finances, and accessing health care information, the risk of fraud and identity theft increases.

[0004] For many years, enterprises have used strong authentication to secure employee and business-partner access to corporate networks and applications. The risk of enabling unauthorized access to corporate assets justified the investment and change in behavior needed to deploy strong authentication and made for a fairly straightforward risk/reward evaluation for the enterprise. However, because these enterprise solutions were designed for lower volume deployments, utilizing them for securing consumer applications is not entirely feasible. Scaling these enterprise authentication solutions to millions of users in a cost effective manner is nearly impossible.

2007215180 04 Jun 2010

[0005] Accordingly, there is a need in the art for a system and method to improve identity protection for consumers.

Summary of the Invention

[0005a] According to a first aspect of an embodiment of the invention, there is provided a method for providing identity protection services, comprising:

receiving at a validation server over a network a response from a credential associated with a user, the credential response provided by the user in order to authenticate the user to one of a plurality of sites on the network that accepts the credential as a factor for authentication;

verifying by the validation server the credential response on behalf of the one network site;

receiving at a fraud detection server over the network information in connection with a transaction associated with the user at the one network site; and

evaluating by the fraud detection server the transaction information for suspicious activity based at least in part on information provided to the fraud detection server in connection with one or more transactions at one or more sites on the network other than the one network site.

[0005b] According to a second aspect of an embodiment of the invention, there is provided a system for providing identity protection services, comprising:

a validation server configured to provide an authentication service;

a fraud detection server configured to provide a fraud detection service;

an authentication database communicatively linked to the validation server; and

a fraud detection database communicatively linked to the fraud detection server, wherein

the validation server receives over a network a response from a credential associated with a user, the credential response provided by the user in order to authenticate the user to one of a plurality of sites on the network that accepts the credential as a factor for authentication,

the validation server verifies the credential response on behalf of the one network site,

the fraud detection server receives over the network information in connection with a transaction associated with the user at the one network site, and

the fraud detection server evaluates the transaction information for suspicious activity based at least in part on information provided to the fraud detection server in connection with one or more transactions at one or more sites on the network other than the one network site.

[0005c] Unless the context clearly requires otherwise, throughout the description and the claims, the words "comprise", "comprising", and the like are to be construed in an inclusive sense as opposed to an exclusive or exhaustive sense; that is to say, in the sense of "including, but not limited to".

Brief Description of the Drawings

[0006] FIG. 1 is a block diagram that depicts a system of network-based authentication and fraud detection services in accordance with an embodiment of the present invention.

[0007] FIG. 2 is a flow chart that depicts a process for providing authentication and fraud detection services in accordance with an embodiment of the present invention.

[0008] FIG. 3 is a flow chart that depicts a two-phase fraud detection process in accordance with an embodiment of the present invention.

[0009] FIG. 4 is a graph upon which a clustering algorithm may be applied in accordance with an embodiment of the present invention.

[0010] FIG. 5 is a block diagram that depicts a bulk provisioning process in accordance with an embodiment of the present invention.

[0011] FIG. 6 is a block diagram that depicts a computing device in accordance with an embodiment of the present invention.

Detailed Description

[0012] The present invention addresses the deficiencies of current solutions by providing to a network of enterprises both authentication and fraud detection services that are hosted by a third party service provider. These services minimize costs and maximize security by sharing intelligence and resources among the network of enterprises that utilize the hosted services. The service provider is able to share authentication credentials among the participating enterprises utilizing the hosted authentication services, and is able to share fraud intelligence (e.g., fraud data and signatures) among the participating enterprises utilizing the hosted fraud detection services. This approach combats digital identity theft on behalf of both consumers and online services without sacrificing the convenience of everyday web lifestyles.

[0013] FIG. 1 depicts a system of network-based authentication and fraud detection services in accordance with an embodiment of the present invention. A third party service provider (100) provides an authentication service (110) and fraud detection service (120) to a number of sites (160, 162, 164, 166) on a network (130) that rely on the service provider (100) for those services (110, 120). These relying parties (160, 162, 164, 166) engage in these services (110, 120) to protect the identity of an end user (170) who may desire to transact with one of the relying parties (164).

[0014] Information stored in a database (115) used by the authentication service (110) may be used by the fraud detection service (120). Similarly, information stored in a database (125) used by the fraud detection service (120) may be used by the authentication service (110).

[0015] The relying parties (160, 162, 164) that utilize the hosted authentication service (110) are considered part of a shared authentication network (140), and the relying parties (162, 164, 166) that utilize the hosted fraud detection service (120) are considered part of a fraud intelligence network (150).

[0016] In connection with the hosted authentication service (110), each party in the shared authentication network (140) accepts the same authentication credentials as other participating members of the network. This enables end users

to utilize a single authentication credential, no matter the form (e.g., OATH-compliant), across any sites of the participating network members. This helps solve the "necklace" problem that occurs when an end user needs a separate credential to transact with different relying parties.

[0017] A credential refers to any electronic device or document used for authentication purposes. The value provided by a credential for validation is referred to as a credential response (e.g., an OTP ("One-Time Password") value, a digital signature, or a response to a challenge-response query). For example, an OTP token (sometimes just called a token) is a hardware device credential that generates a unique code on demand that is usually used, for example, as a second factor for authentication.

[0018] Second factor authentication refers to authenticating something that the user has or something the user is (the second factor) rather than or in addition to something the user knows (the first factor). In a system that employs first and second factor authentication, if an attacker steals only a first factor, the attacker would not be able to forge the second factor and would be unable to authenticate. If an attacker steals the second factor, the attacker would not know the first factor and would be unable to authenticate.

[0019] There may be many different types of secondary factors, such as hardware tokens, digital certificates, and biometric devices. Additionally, an authentication service may require more than two factors. For example, a system might require a pass phrase, digital certificate, and thumbprint sensor, combining something the user knows, something the user has, and something the user is.

[0020] A second factor network is an elegant way to facilitate using a single, easy to use device. An end user receives a single device that works the same way everyplace in the network. A user simply registers the device with a service that supports the second factor network, and is ready to authenticate. If the user loses or breaks the device, the user contacts the issuer of the device and each relying party learns of the change in status. Service providers do not have to worry about managing end user credentials and devices, but simply contact the network.

[0021] In connection with the hosted fraud detection service (120), each party in the fraud intelligence network (150) shares fraud intelligence (e.g., web browser headers, IP addresses, etc.) to further maximize identify protection. By sharing transaction information from across the network (150), the fraud detection service (120) can compare patterns of behavior across the participating sites in real time, and help detect and stop attacks that could not be detected with data from a single site. The service (120) does not require personally identifiable information to detect fraud, but can use unique pseudonyms to identify end users across the different sites.

[0022] The service provider 100 may query external sources to gain network level intelligence derived apart from the fraud intelligence network information. Such intelligence may involve information associated with the DNS infrastructure of the Internet, such as IP geolocation data, connection type, network provider, GPS data, Home Location Register data, calling and called telephone (land-based and/or cellular) data, etc.

[0023] The fraud detection service (120) is therefore able to better combat criminals on the internet who use many different mechanisms to capture personal information, such as phishing web sites, key loggers, false store fronts, and database theft. Often, criminals try to use the same information on multiple web sites, testing login information by trial and error, establishing multiple fraudulent accounts, or other malicious activities.

[0024] FIG. 2 depicts a process for network-based authentication and fraud detection in accordance with an embodiment of the present invention. When a relying party (164) requires (step 200) a credential to authenticate an end user (170), the user (170) provides (step 210) a credential response associated with a credential possessed by the user (170) to be validated (step 220) by an authentication service (110).

[0025] In one embodiment of the present invention, the user (170) may provide the credential response to the relying party (164), who then checks the information with the authentication service (110) via a backend integration. In another embodiment, the relying party (164) may redirect the user (170) to the

authentication service (110) to enter the credential response. In this embodiment, the authentication service (110) creates a digitally signed assertion - stating whether the attempt was good or bad - and encodes it into a short ASCII string that can be attached to a URL to be passed back to the relying party (164) using an http redirect. In yet another embodiment, the relying party (164) may utilize AJAX (Asynchronous Javascript and XML) so that, instead of redirecting the user's web browser to different web pages, Javascript on the relying party's (164) page is used to forward the credential response to the authentication service (110) (e.g., via an XMLHttpRequest call) and receive the resulting assertion.

[0026] The relying party (164) then monitors (step 230) transactions associated with the user (170), which may include a login, purchase, click-thru, or any other activity by the user (170) on the relying party's (164) site, and provides information associated with the transactions to the fraud detection service (120) to be evaluated (240) for suspicious activity. To improve security, the fraud detection service (120) evaluates the transaction information for suspicious activity based at least in part on other transaction information provided to the fraud detection service (120) by the fraud intelligence network (150) sites.

[0027] FIG. 3 is a flow chart that depicts a two-phase fraud detection process in accordance with an embodiment of the present invention. First, a user (170) provides (step 300) login credentials to a relying party (164) for validation (step 310). If the credentials are bad, the login is refused (step 320), and if the credentials are good, then the relying party (164) forwards (step 330) information associated with the user's login to a fraud detection service (120).

[0028] The fraud detection service (120) checks (step 340) for suspicious activity, and if no suspicious activity is found, the transaction passes (step 350), the relying party (164) is informed of the decision, and the user (170) is allowed (step 360) to log in.

[0029] If, on the other hand, the primary check reveals suspicious activity, then the fraud detection service (120) proceeds (step 370) to use more sophisticated, complex, and invasive techniques to validate that the credential is legitimate. After

this secondary check, the fraud detection service (120) decides if the transaction is fraudulent or legitimate.

[0030] The primary fraud checks may be based on properties of the transaction, properties of the user account, and transaction history. No human intervention is required; these checks may be completely automated. More importantly, no extra steps are added to the process.

[0031] The secondary fraud checks add additional steps to the process. The fraud detection service (120) may require a telephone, email, or SMS confirmation of the user's identity. Alternately, the system may ask additional challenge/response questions of the user (170). The purpose of these checks is to provide additional information to validate the user's identity. If the secondary checks succeed, the fraud check succeeds (step 350), and the user is allowed to log in (step 360).

[0032] If the secondary checks fail, the fraud check fails (step 380) and the fraud detection service (120) reports the failure to the relying party (164). The relying party (164) may refuse (step 320) the login request, and may choose to refer the customer to customer service for resolution.

[0033] In an embodiment of the present invention, information associated with a refused login based on step 310 may also be sent to the fraud detection service (120) by the relying party (164).

[0034] In order to check for suspicious activity, the fraud detection service (120) may be fed information about each transaction. Using a scoring model or rules, the service (120) outputs a decision. Each decision, and all transaction details, may then be saved to a transaction log. Periodically, an Extraction Translation and Loading (ETL) process may be used to calculate some information for a transaction history database (125). Some details about recent transactions may also be saved directly to the transaction history database (125) (e.g., simple, easy to calculate information). A scoring engine may also query a database containing information from external sources (such as IP geolocation data, GPS data, Home Location Register data, calling and called telephone (land-based and/or cellular) data, etc.) that can be used to enhance decisions.

[0035] The scoring engine is designed to distinguish between good and bad authentication attempts. There are two types of login transactions: legitimate authentication attempts and fraudulent authentication attempts. In order to distinguish between the two, the engine attempts to learn whether a login does not fit a pattern of other legitimate attempts, and whether a login fits the pattern of other fraudulent attempts.

[0036] Over time, a good picture of what a legitimate login attempt looks like for each account can be developed by the engine. For example, suppose that a user in Minnesota uses a token to access his trading account. Over time, it might become evident that he usually logs in only during market hours, only logs in 3-4 times per week, and only logs in from an IP address in the Midwest.

[0037] Any deviation from this pattern is a sign of suspicious activity. For example, the engine will deem suspicious transaction information that shows twenty attempted authentications at midnight EST from Russia. The engine characterizes the usual usage pattern and then looks for deviations from that pattern.

[0038] Other examples of baseline behavior could be based upon the known geolocation of the user, which can be compared to actual location data obtained from a GPS system associated with the user (e.g., embedded in his cell phone, where the interface for logging in is, for example, through the cell phone), Home Location Register information, called number information, etc. Any unusual discrepancy between his known location and these locations could indicate fraud. Furthermore, any discrepancy among these data could indicate fraud. For instance, if the GPS data indicates Minnesota and the Home Location Register data indicates New York, fraud may be suspected and anti-fraud measures implemented.

[0039] A picture of fraudulent login attempts can also be developed by the engine over time. For example, it might become evident that many fraudulent login attempts are through anonymous IP proxies, or from Eastern European countries. It might become evident that fraudulent attempts try to use a token at the wrong web site, or that dictionary attacks are made against a token (e.g., systematically

testing different PIN codes with a token), etc. Rules can be coded to detect and counter practically any kind of fraudulent behavior.

[0040] In order to detect fraud, the fraud detection service (120) needs to collect enough information about each transaction to make a reasonable guess. In order to capture broad enough information, the following fields can be used:

- Token serial number (or token group ID)
- Token type (OTP, PKI, etc.)
- Time of transaction
- IP address of token user
- Web site/System the user is trying to access
- Transaction the user is attempting (i.e., login, purchase, stock trade, etc.)
- Approximate transaction value
- Result of authentication attempt (good or bad OTP, good or bad PIN, wrong site, etc.)

[0041] The fraud detection service (120) also needs to capture deep enough information. This means producing a historical record of transactions, going back at least 90 days and preferably for a year, for example. Over time, summary information could be built (such as the average number of logins per month) that could be used to look for suspicious activity.

[0042] The fraud detection service (120) analyzes a transaction by a policy engine and, depending on the policy, is passed through an anomaly engine which answer with a status (anomaly or not) and a confidence factor (how much the engine is confident in its decision) that is processed back by the policy engine. The following provides an embodiment of the data flow process:

- Data arrives into the system through a data adapter
- The policy engine runs rules that are relevant to the events
- If required, the policy engine passes the events to the anomaly engine for anomaly detection
- The policy engine receives back a result which is structured as a status (is anomaly?) and confidence factor
- According to the confidence factor and the status, the policy engine issues additional events, including user defined actions and internal analytics

[0043] Each rule may have a condition and a list of actions. For example, a condition can be that an event occurred, data in a graph changed, fact value changed, etc. An action can be to change data in a graph, set a fact value, send an email, run a script, etc. The rules may be grouped into policies. Each policy may have a Name, an attribute (Enable/Disable) and a Durability (schedule of when the policy is active). Policies may be logically stored in directories.

[0044] In addition to providing functionality around setting filters based around how anomalous and how confident the engine is in the decision, the fraud detection service (120) may use its determinations for further increasing accuracy. For example, if a transaction is tagged as anomalous, even with a high anomaly score and confidence factor, the system can increase its accuracy by comparing the transaction against a cluster of known fraudulent transactions or known "not" fraudulent transactions.

[0045] In order to achieve this unsupervised learning, the fraud detection service (120) may utilize clustering algorithms in its anomaly engine to decide which of the user's actions correspond to natural behavior and which are exceptional, without any assistance.

[0046] The clustering algorithm may be based on the ROCK hierarchical clustering algorithm (RObust Clustering using linKs), which is an agglomerative hierarchical clustering algorithm based on the notion of neighbors and links as follows.

[0047] Two data elements are considered as neighbors if our similarity upon a domain expert or similarity matrix exceeds a certain threshold. At first, all n data elements are mapped to n clusters respectively. Then, with each iteration, the engine merges between the two closest clusters such that both clusters fulfill the maximum value of Link(C_i,C_j), for any pair of clusters C_i and C_j. The metric Link(C_i,C_j) represents the number of common neighbors between every element in the first cluster to every element in the second one.

[0048] This measure is normalized by the number of potential neighbors in both clusters, so that a large cluster will not swallow every other cluster and end up with all the elements. Grouping the data elements using links injects global knowledge

into the clustering process, forming an optimal division between the elements. Thus, the formed clusters aren't too large or too small, and the clusters contain elements that are relatively similar one to another.

[0049] The engine utilizes enhancements to the ROCK algorithm that adapt it to the overall anomaly detection process. Namely, the enhancements significantly improve the clustering phase's execution time and transform the ROCK's ability of finding clusters to the ability of finding anomalies. Additional to these enhancements, the engine utilizes enhancements on the algorithmic level as follows.

[0050] Like other clustering algorithms, the ROCK also expects an argument that determines the number of clusters to generate. The enhanced algorithm, on the other hand, produces the real amount of clusters, representing each of the user's behavioral patterns, as they actually appear within the data.

[0051] Additionally, the algorithm introduces the notion of clustering execution levels, which allow for different clustering configurations to be defined for various situations. If, for example, the anomaly detection process is started with a relatively sparse data set, then engine may want to activate the clustering phase with reduced similarity thresholds, since the number of common neighbors between pairs of data elements is bound to be small.

[0052] This enables the engine to perform fraud detection at early stages of the data collection, without generating false positives or false negatives. In each execution level, the minimum number of transactions, similarity threshold, confidence factor and the participating attributes can be defined.

[0053] FIG. 4 depicts a graph upon which the enhanced clustering algorithm may be applied in accordance with an embodiment of the present invention.

First Step:

[0054] Let S be the similarity function. Compute S(x, y) for all elements.

[0055] Similarity is defined in this example as being "close" to each other or being connected.

Second Step:

[0056] Build the neighbor matrix:

$$M(x,y) = 1 \text{ if } S(x,y) > T \text{ a certain Threshold value.}$$

[0057] In this example, for instance: M(e,d) = 1 and M(d,f) = 1 because e and d are close, and d and f are connected; but M(a,b) = 0 because they are far apart and not connected.

[0058] The full Matrix is represented in TABLE 1:

TABLE 1

	a	b	c	d	e	f
a	1	0	1	1	0	1
b	0	1	1	0	0	0
c	1	1	1	0	0	0
d	1	0	0	1	1	1
e	0	0	0	1	1	0
f	1	0	0	1	0	1

Third Step:

[0059] Create the Link Matrix.

[0060] The number of common neighbors are calculated for each pair (x,y) of elements.

[0061] So for example upon taking a and c in TABLE 2:

TABLE 2

a	1	0	1	0	0	1
c	1	1	1	0	0	0

[0062] The number of common neighbors is 2. The link matrix for this example is shown IN TABLE 3:

TABLE 3

	a	b	c	d	e	f
a	-					
b	1	-				
c	2	2	-			
d	2	0	0	-		
e	0	0	0	1	-	
f	2	0	1	0	1	-

Last Step:

[0063] Criterion functions

- Maximize the sum of Link(x, y) for x and y belonging to the same cluster
- Minimize the sum of Link(x, y) for x and y belonging to different clusters

[0064] Intuitively, the idea is to be sure that within a cluster, elements have as many common neighbors as possible while at the same time, these elements are as "dissimilar" as possible from the elements in other clusters.

[0065] Based on these metrics, a goodness measure is also calculated to decide on whether to merging the clusters or not – the generalization from points to clusters is logical.

[0066] Let k be the parameter that is used to specify to the system the number of clusters to reach "possibly" – remember that k is not an absolute limit, and the system can try to merge more clusters but it will not "insist" on merging once k is reached.

[0067] Assuming k = 3, (a, c, d, f) will be clustered while b and e will remain separate.

[0068] If k = 2, it is likely that a large cluster (a, c, d, e, f) is formed, while b remains separate since it has only 1 connection to c and it is not as "close" (visual distance here as similarity) as e to d, and d being connected to a and f.

[0069] This simplified example serves to explain the main principles of the enhanced clustering algorithm implemented by the anomaly engine.

[0070] As shown in FIG. 5 in accordance with an embodiment of the present invention, a credential issuer (500), such as the service provider (100), may provide bulk back-end generation of seeds and their secure transport (530) to a token manufacturer (510) upon request (520). Utilizing a bulk provisioning protocol enables the sending of pre-provisioned tokens – devices that are ready to be activated and used – to users.

[0071] The complexity of generating a secret known only by the token or device – used to generate the OTP - and the back-end service – used to validate the OTP - is handled by the issuer (500) and the trusted partner (510) who is manufacturing a specific token or OATH compatible device, for example. An issuer- supplied application – Token Manufacturing Utility (TMU) - may be installed and integrated in a manufacturing facility to allow requests of batches of seeds that are later integrated in the OTP generating devices. This way the device manufacturer (510) can leverage existing processes, without increasing the complexity of the device itself other than the functionality needed to generate and provide for consumption the OTP itself.

[0072] In an embodiment of the present invention, the bulk provisioning protocol may be described as follows:

- TMU generates a key pair and token ID for each token
  - the TMU generates a random key pair, which includes a public key, for each token ID
  - this public key is used transparently as a second parameter in each enrollment request made by the provision command
  - TMU can enroll for a certificate for each token, with the required token IDs as parameters
- an OTP shared secret is always requested for each token ID
  - optionally, an administrative shared secret may be requested for each token ID as well

[0073] TMU may use the Registration Authority key to negotiate the establishment of an authenticated SSL channel. This channel persists until the enrollment process for each token is completed.

[0074] The bulk provisioning protocol flow may be described in an embodiment of the invention as follows:

- TMU connects to the issuer's provisioning service and enrolls an for OTP certificate and optionally an administrative certificate for each token ID presented
- the issuer (500) returns the required certificates and shared secret for each token, in encrypted form
- the issuer (500) stores a copy of the shared secrets at its site; OTP shared secrets are used to calculate the OTP values that are used to authenticate users; an administrative shared secret is used when resetting a lost password
- the issuer (500) returns the certificates
- TMU stores the certificates and shared secrets in encrypted form in a local keystore

[0075] After shared secrets are received from the issuer (500), the token manufacturer (510) embeds them in the correct tokens. The following process may be utilized in accordance with an embodiment of the invention:

- extract and decrypt a token ID and shared secret from the local keystore for each token using a list command
- decrypt the shared secret for each token ID output by the list command, using a secure method
- embed the shared secret in the correct token using manufacturing process

[0076] FIG. 6 illustrates the components of a basic computing device in accordance with an embodiment of the present invention, which may include a server running the authentication service (110) or fraud detection service (120), for example. The computing device may be a personal computer, workstation, server, or any other type of microprocessor-based device. The computing device may include one or more of a processor (610), input device (620), output device (630), storage (640), and communication device (660).

[0077] The input device (620) may include a keyboard, mouse, pen-operated touch screen or monitor, voice-recognition device, or any other device that provides

input. The output device (630) may include a monitor, printer, disk drive, speakers, or any other device that provides output.

[0078] The storage (640) may include volatile and nonvolatile data storage, including one or more electrical, magnetic or optical memories such as a RAM, cache, hard drive, CD-ROM drive, tape drive or removable storage disk. The communication device (660) may include a modem, network interface card, or any other device capable of transmitting and receiving signals over a network. The components of the computing device may be connected in any manner, such as via electrical bus or wirelessly.

[0079] The software (650), which may be stored in the storage (640) and executed by the processor (610), may include, for example, the application programming that embodies the functionality of the present invention (e.g., as embodied in the authentication service (110) and fraud detection service (120)). The software (650) may include a combination of client applications and enterprise servers such as an application server and a database server.

[0080] Communications may occur over any type of network, which may implement any communications protocol, which may be secured by any security protocol. Network links may include telephone lines, DSL, cable networks, T1 or T3 lines, wireless network connections, or any other arrangement that implements the transmission and reception of network signals.

[0081] The computing device may implement any operating system, such as Windows, Linux or UNIX. The software (650) may be written in any programming language, such as C, C++, Java, Visual Basic and/or SQL. In various embodiments, application software embodying the functionality of the present invention may be deployed on a standalone machine, in a client/server arrangement or through a Web browser as a Web-based application or Web service, for example.

[0082] Several embodiments of the invention are specifically illustrated and/or described herein. However, it will be appreciated that modifications and variations of the invention are covered by the above teachings and within the purview of the appended claims without departing from the spirit and intended scope of the invention.

[0083] For example, software functionality that implements the present invention such as the authentication service (110) and fraud detection service (120) may comprise several discrete modules that together still provide the same functionality, data specified in the illustrated databases may be spread over several database partitions, databases and/or systems, and the data and flow diagrams of FIGS. 2-3 and 5 may encompass combined steps or several intermediate steps that do not detract from the higher level functionality described therein.

2007215180 04 Jun 2010

THE CLAIMS DEFINING THE INVENTION ARE AS FOLLOWS:-

1. A method for providing identity protection services, comprising:

receiving at a validation server over a network a response from a credential associated with a user, the credential response provided by the user in order to authenticate the user to one of a plurality of sites on the network that accepts the credential as a factor for authentication;

verifying by the validation server the credential response on behalf of the one network site;

receiving at a fraud detection server over the network information in connection with a transaction associated with the user at the one network site; and

evaluating by the fraud detection server the transaction information for suspicious activity based at least in part on information provided to the fraud detection server in connection with one or more transactions at one or more sites on the network other than the one network site.

2. The method of claim 1, wherein the validation server utilizes transaction information provided by the fraud detection server in connection with verifying the credential response provided by the user.

3. The method of claim 1 or claim 2, wherein the fraud detection server utilizes verification information provided by the validation server in connection with evaluating the user's transaction information for suspicious activity.

4. The method of claim 1 or claim 2, wherein the fraud detection server evaluates the transaction information for suspicious activity based at least in part on other information not provided to the fraud detection server in connection with the one or more transactions at the one or more sites on the network other than the one network site.

5. The method of claim 4, wherein the other information is queried from a database associated with the DNS infrastructure of the Internet.

6. The method of claim 5, wherein the other information includes IP geolocation data.

7. A system for providing identity protection services, comprising:

a validation server configured to provide an authentication service;

a fraud detection server configured to provide a fraud detection service;

an authentication database communicatively linked to the validation server; and

a fraud detection database communicatively linked to the fraud detection server, wherein

the validation server receives over a network a response from a credential associated with a user, the credential response provided by the user in order to authenticate the user to one of a plurality of sites on the network that accepts the credential as a factor for authentication,

the validation server verifies the credential response on behalf of the one network site,

the fraud detection server receives over the network information in connection with a transaction associated with the user at the one network site, and

the fraud detection server evaluates the transaction information for suspicious activity based at least in part on information provided to the fraud detection server in connection with one or more transactions at one or more sites on the network other than the one network site.

8. The system of claim 7, wherein the validation server utilizes transaction information provided by the fraud detection server in connection with verifying the credential response provided by the user.

9. The system of claim 7 or claim 8, wherein the fraud detection server utilizes verification information provided by the validation server in connection with evaluating the user's transaction information for suspicious activity.

10. The system of claim 7 or claim 8, wherein the fraud detection server evaluates the transaction information for suspicious activity based at least in part on other information not provided to the fraud detection server in connection with the one or more transactions at the one or more sites on the network other than the one network site.

2007215180 04 Jun 2010

11. The system of claim 10, wherein the other information is queried from a database associated with the DNS infrastructure of the Internet.

12. The system of claim 11, wherein the other information includes IP geolocation data.

13. A method for providing identity protection services substantially as herein described with reference to any one of the embodiments of the invention illustrated in the accompanying drawings and/or examples.

14. A system for providing identity protection services substantially as herein described with reference to any one of the embodiments of the invention illustrated in the accompanying drawings and/or examples.

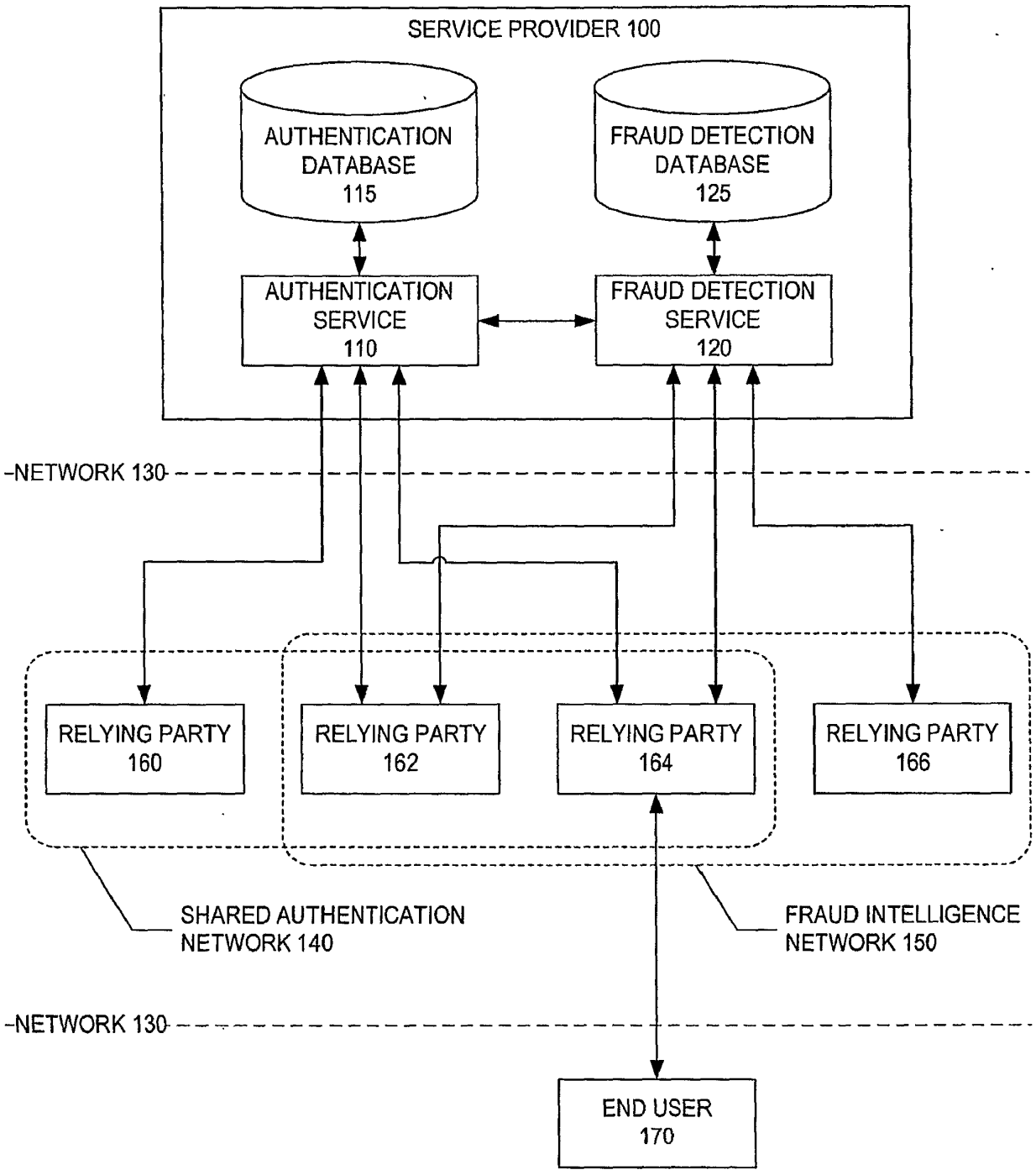

SERVICE PROVIDER 100
AUTHENTICATION DATABASE 115
FRAUD DETECTION DATABASE 125
AUTHENTICATION SERVICE 110
FRAUD DETECTION SERVICE 120
NETWORK 130
RELYING PARTY 160
RELYING PARTY 162
RELYING PARTY 164
RELYING PARTY 166
SHARED AUTHENTICATION NETWORK 140
FRAUD INTELLIGENCE NETWORK 150
NETWORK 130
END USER 170

FIG. 1

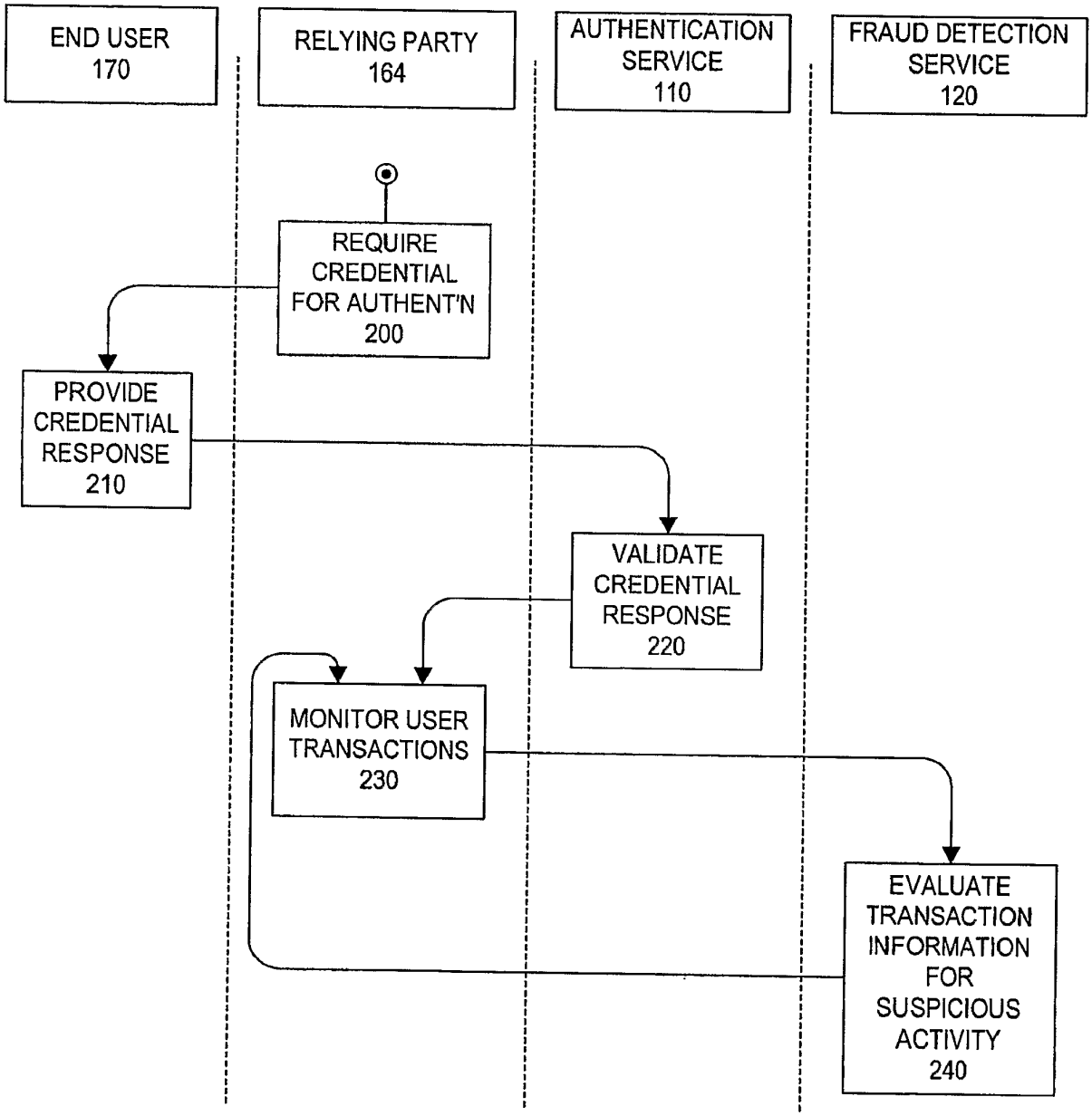
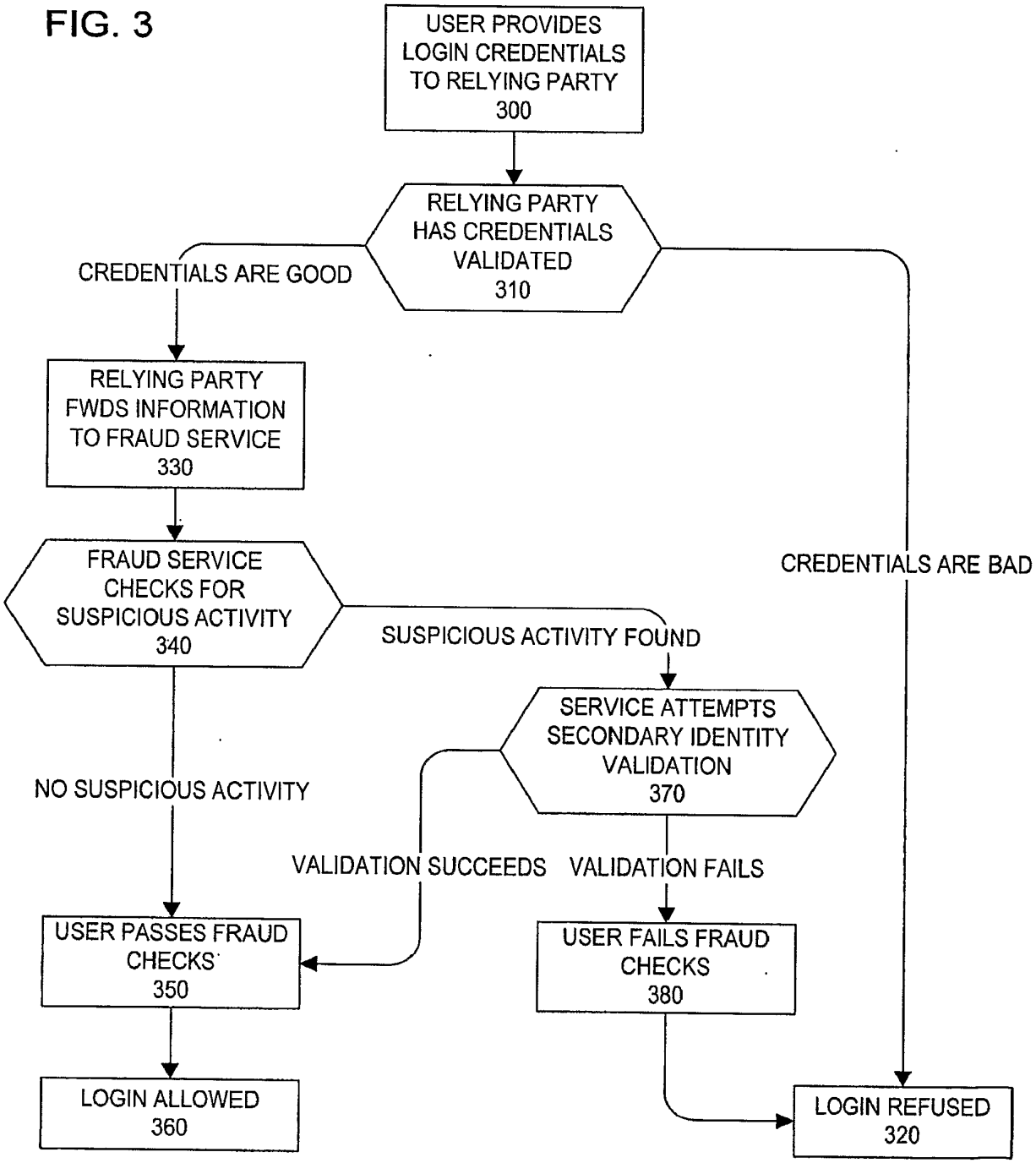

END USER
170
RELYING PARTY
164
AUTHENTICATION SERVICE
110
FRAUD DETECTION SERVICE
120
REQUIRE CREDENTIAL FOR AUTHENT'N
200
PROVIDE CREDENTIAL RESPONSE
210
VALIDATE CREDENTIAL RESPONSE
220
MONITOR USER TRANSACTIONS
230
EVALUATE TRANSACTION INFORMATION FOR SUSPICIOUS ACTIVITY
240

FIG. 2

FIG. 3


USER PROVIDES LOGIN CREDENTIALS TO RELYING PARTY 300
RELYING PARTY HAS CREDENTIALS VALIDATED 310
CREDENTIALS ARE GOOD
CREDENTIALS ARE BAD
RELYING PARTY FWDS INFORMATION TO FRAUD SERVICE 330
FRAUD SERVICE CHECKS FOR SUSPICIOUS ACTIVITY 340
SUSPICIOUS ACTIVITY FOUND
NO SUSPICIOUS ACTIVITY
SERVICE ATTEMPTS SECONDARY IDENTITY VALIDATION 370
VALIDATION SUCCEEDS
VALIDATION FAILS
USER PASSES FRAUD CHECKS 350
USER FAILS FRAUD CHECKS 380
LOGIN ALLOWED 360
LOGIN REFUSED 320

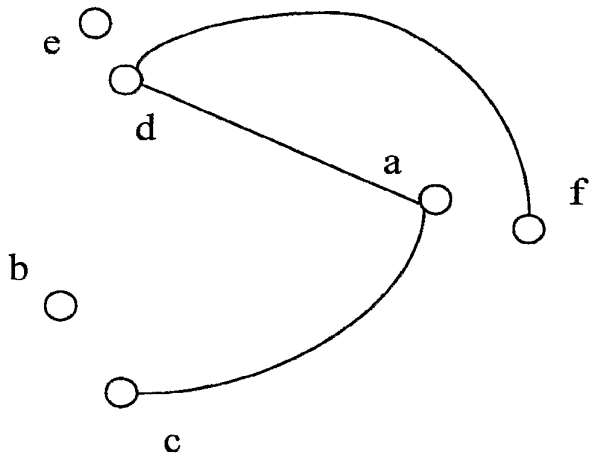


FIG. 4

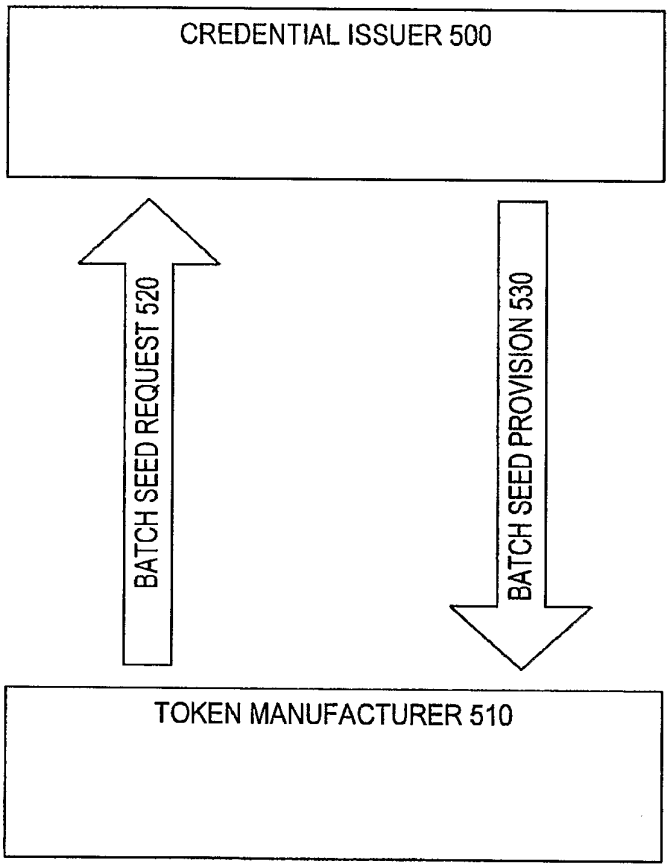

CREDENTIAL ISSUER 500
BATCH SEED REQUEST 520
BATCH SEED PROVISION 530
TOKEN MANUFACTURER 510

FIG. 5

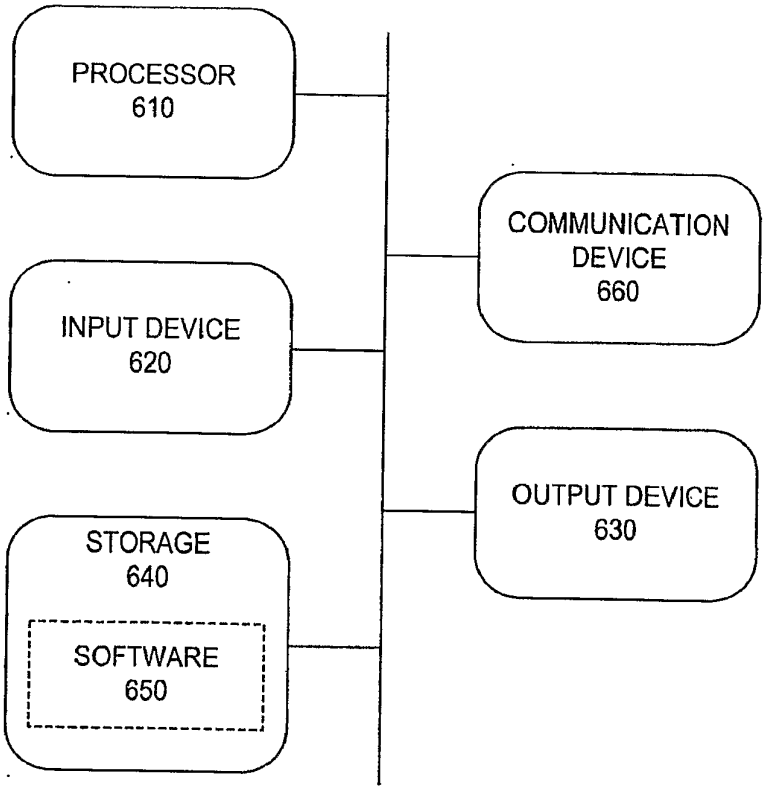

PROCESSOR
610
INPUT DEVICE
620
STORAGE
640
SOFTWARE
650
COMMUNICATION
DEVICE
660
OUTPUT DEVICE
630

FIG. 6