PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 :
H04Q 7/00

A1

(11) International Publication Number: **WO 96/41488**

(43) International Publication Date: 19 December 1996 (19.12.96)

(21) International Application Number: PCT/US96/10096

(22) International Filing Date: 7 June 1996 (07.06.96)

(30) Priority Data:
08/481,021 7 June 1995 (07.06.95) US

(71) Applicant: THE DICE COMPANY [US/US]; P.O. Box 60471, Palo Alto, CA 94306-0471 (US).

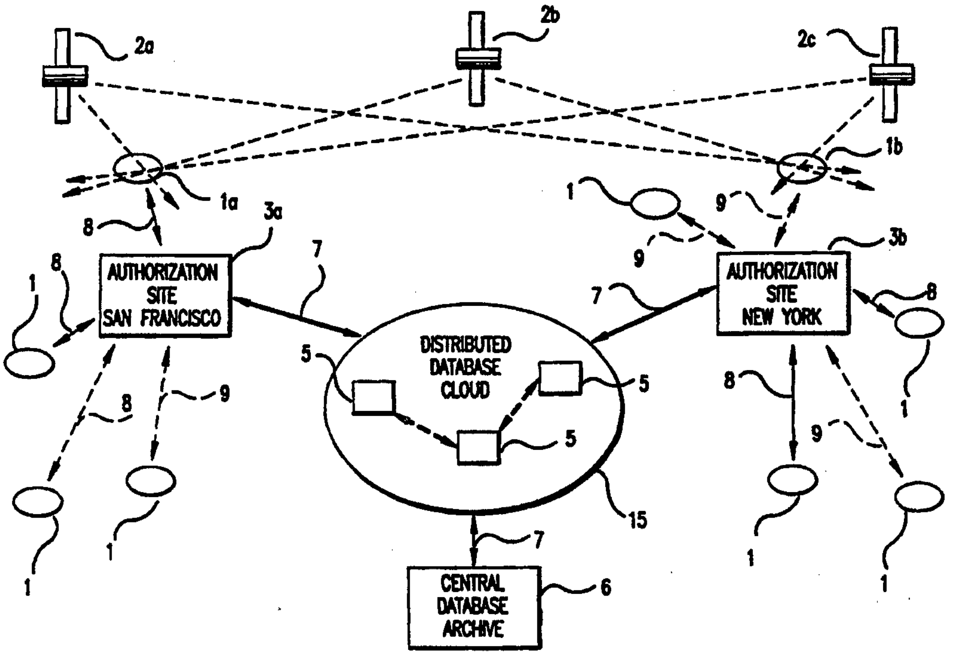
(72) Inventor: COOPERMAN, Marc, S.; 2929 Ramona, Palo Alto, CA 94306 (US).

(74) Agents: ALTMILLER, John, C. et al.; Kenyon & Kenyon, 1025 Connecticut Avenue, N.W., Washington, DC 20036 (US).

(81) Designated States: CA, CN, JP, KR, SG, European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: FRAUD DETECTION SYSTEM FOR ELECTRONIC NETWORKS USING GEOGRAPHICAL LOCATION COORDINATES


2a
2b
2c
1b
1a
1
9
8
3a
3b
7
AUTHORIZATION SITE SAN FRANCISCO
AUTHORIZATION SITE NEW YORK
DISTRIBUTED DATABASE CLOUD
5
15
CENTRAL DATABASE ARCHIVE
6

(57) Abstract

An active fraud detection and fraud prevention system for electronic networks which gathers and collates location information for each of a number of uniquely identified terminal devices (1) on the network. The system analyzes the location information in real time, on a transaction by transaction basis, to determine the likelihood that a terminal device (1) has been cloned or illegally duplicated. The system then automatically rejects transactions for devices (1) it considers likely to be cloned, alerts human operators, and keeps records of suspicious transaction attempts.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AM	Armenia
AT	Austria
AU	Australia
BB	Barbados
BE	Belgium
BF	Burkina Faso
BG	Bulgaria
BJ	Benin
BR	Brazil
BY	Belarus
CA	Canada
CF	Central African Republic
CG	Congo
CH	Switzerland
CI	Côte d'Ivoire
CM	Cameroon
CN	China
CS	Czechoslovakia
CZ	Czech Republic
DE	Germany
DK	Denmark
EE	Estonia
ES	Spain
FI	Finland
FR	France
GA	Gabon
GB	United Kingdom
GE	Georgia
GN	Guinea
GR	Greece
HU	Hungary
IE	Ireland
IT	Italy
JP	Japan
KE	Kenya
KG	Kyrgystan
KP	Democratic People's Republic of Korea
KR	Republic of Korea
KZ	Kazakhstan
LI	Liechtenstein
LK	Sri Lanka
LR	Liberia
LT	Lithuania
LU	Luxembourg
LV	Latvia
MC	Monaco
MD	Republic of Moldova
MG	Madagascar
ML	Mali
MN	Mongolia
MR	Mauritania
MW	Malawi
MX	Mexico
NE	Niger
NL	Netherlands
NO	Norway
NZ	New Zealand
PL	Poland
PT	Portugal
RO	Romania
RU	Russian Federation
SD	Sudan
SE	Sweden
SG	Singapore
SI	Slovenia
SK	Slovakia
SN	Senegal
SZ	Swaziland
TD	Chad
TG	Togo
TJ	Tajikistan
TT	Trinidad and Tobago
UA	Ukraine
UG	Uganda
US	United States of America
UZ	Uzbekistan
VN	Viet Nam

Fraud Detection System for Electronic Networks Using Geographical Location Coordinates

Background of the Invention

In recent years a number of electronic communications networks, computer networks, and on-line systems have proliferated. These systems all deliver some value in goods or services to the subscriber, who pays fees for both the usage of the system and the value of goods or services purchased. These systems include some method of billing the subscriber, the intent of which is to attribute to that subscriber the charges associated with his/her authorized use of the system, and thus generate a liability on the part of the subscriber. In the case of electronic networks like cellular phone systems, which are delivered to the subscriber in small portable devices, an identification code is integrated into the subscriber's device, in order to identify that subscriber, who is typically remote from the billing authority. In the case of computer networks and on-line services, a code which is attributed to each user serves as the billing identification. In this case, the subscriber must input the code manually to validate each purchase. These codes may be credit card numbers, allowing the service provider to directly debit the accounts of these subscribers. In other cases, passwords may be used. Note that credit card numbers and passwords may also be added to electronic networks like cellular phone network to provide alternate billing options.

These systems all share a common problem. Possession of the ID code (or device, which implies possession of the ID code) of a subscriber allows an unauthorized individual to charge goods and services to the account of that subscriber, thus perpetrating acts of fraud on the system. A stolen cellular phone, a cloned phone, or a stolen credit card number or other password will allow such fraud, typically until discrepancies are noticed upon the next account statement. In some extreme cases, sudden inordinate charges, or charges incurred from widely disparate geographical points of sale (using credit cards) may alert the billing authority to a problem more expediently. Note that there is inherent geographical information included in the address/location of the commercial entity who generates a charge on a credit card. The credit card company may use this information to spot a misappropriated card number, if the card is used in locations deemed unusual based on the previous charges compiled by the legitimate card holder. Such information is not necessarily available or reliable on computer systems.

Computer networks in particular, and possibly electronic and telecommunication networks, like that of cellular phones, do not include or associate any geographical data on the point of sale with such transactions in the billing database. Computer networks pose particular problems to the usefulness of such information, since an individual may typically connect to and operate computers from anywhere in the world, with minimal effort. Tracking an individual on a computer network to an actual geographical location can be quite difficult, especially if they do not want to be located. Even telecommunications networks which may offer "trace" capabilities, like the phone system, can be fooled by individuals with the technical know-how to disguise their signal.

US Patent 5,327,144, issued to Stilp, et al., discloses a "Cellular Telephone Location System". Stilp discloses a system and method for establishing the location of a cellular handset unit, using triangulation data from 3 or more ground-located cell site antennae, using information from the Global Positioning System (GPS). The triangulation data is transmitted from the cell site, to a central site, and finally to a database, which may be co-located with the central site. Finally, Stilp details an algorithm for collating the data from said 3 or more cell sites, determining handset location from such data, and storing this information in the database. The patent basically provides a method by which an existing cellular telephone network may be adapted to perform GPS location calculations.

Previous systems for prevention of fraud in electronic services focused on methods for tracking the fraudulent device after the billing authority has determined that fraud is likely or is definitely being committed. Such methods are termed herein as "passive" fraud detection systems. Such a system is detailed, e.g., in US Patent 5,335,278, "Fraud Prevention System and Process for Cellular Mobile Telephone Systems", to Matchett, et al. Matchett describes a system whereby the central cell sites, as described in Stilp, et al., can gain access to a list, describing user authorization data, maintained by many or all cellular service providers. An improvement detailed in Matchett et al. is the ability of each cell site to check an incoming request for service against this list in real-time, to determine, before service is granted, whether the request is from a legitimate user. If the ID codes in the user's handset were either a) not on the list or b) listed as stolen, the request for service is denied, and the billing authority could presumably use the methods of Stilp et al. to gather location data. Matchett et al. also describes a method of distributing this authorization data to remote cell sites via a satellite downlink.

While Stilp et al. relies on the existing cellular phone system infrastructure to make use of cell-site broadcast/receive antennae, in order to calculate a global position, there is a need for a system which can extend its use beyond cellular phones. One possibility is by the inclusion in the terminal hardware of GPS receiving circuits to tap into the Global Positioning Satellites in position around the planet in order to address the problem of fraud.

The prior art relies on the periodic distribution of a list of good and bad cellular IDs, maintained manually by a billing authority, which is possibly incomplete, to individual cell sites which handle requests for service. There is a need for a system which details links between approval sites to update and share information collected automatically in the course of processing transactions in a central database. While the prior art relies on a simple comparison of serial numbers versus valid and stolen numbers to identify requests from known stolen Ids or fictitious IDs, the system described herein may also check such a list but it also compares global coordinates associated with each request against an accumulated list of past transaction information from the same ID. The present system then determines based on the timing of shifts in location coordinates for a given device whether such a request is from a device that has likely been cloned. So, whereas the prior art aims to stop the granting of service to stolen IDs, the system disclosed herein aims to go a step further and actually identify stolen IDs, using the collation of location data from multiple transactions.

Summary of the Invention

The present invention is directed towards improving the detection of fraud on such electronic systems by causing to be associated with a registration record additional information comprised of a time stamp indicating the time the transaction occurred, and location coordinates generated by the terminal device and integrated into the transaction protocol. The present invention is also intended to be used in more general purpose computing devices incorporated into networks (such as LAN and WAN) for the purposes of adding an additional layer of security to more traditional computer to computer transaction security protocols. Such computing devices could be retrofitted with hardware to provide the location information. One possibility is to provide GPS data. Specifically, the present invention is meant to incorporate location data at a very low level of the protocol to add reliable geographical positioning information to computer networks.

In a first embodiment of the present invention, hardware is added to a computing or other electronic device. Typical devices are those used to incur liability or conduct transactions for purpose of information exchange, or request of service, such as a cellular phone handset or a computer terminal. The hardware can receive signals from the various Global Position System satellites in orbit about the Earth. The signals allow the hardware to determine to a high degree of accuracy (9 meters or less) the exact position on the surface of the planet which the device occupies. The hardware, which is deployed in tamperproof packaging within the device, directly relays the GPS information to the computing system itself, for transmission to a billing authority.

The inclusion of location receiving hardware in the computing access device can add a new dimension of geographical location, which is not inherent in transactions between computer systems, to the transaction information. When location is used together with timing information, and the assumption that each device ID code is unique (i.e., there can be only 1 authorized device which generates a specific code), and multiple transactions attributed to the same device ID are collated by the billing authority, transactions in which authorization was impossible or highly improbable are immediately apparent to the billing authority. For instance, two transactions could not occur simultaneously in two disparate locations for the same device ID. Similarly, a transaction conducted at 9 am EST in New York City is suspicious when viewed in the context of the same device incurring a transaction at 6:30 am Pacific time on the same day. In such cases the validity of the registered device number involved in such transactions could be immediately suspended, pending further investigation, thus preventing additional fraud. If it is clear a device ID has been cloned, the device ID could be permanently retired, and the legitimate owner issued a new device with a fresh ID.

The invention herein disclosed improves the state of the art by taking an "active" approach to fraud detection. This new system automatically determines on a transaction by transaction basis whether each transaction is suspicious. This leads to faster detection of fraud, and thus fewer instances of fraud and decreased monetary losses that result from it. In addition, the methods described as part of the new invention apply beyond the realm of cellular phone service to any remotely delivered electronic service which depends on a piece of terminal hardware.

The present invention represents an improvement over the prior art, in providing a method and apparatus for the active detection of fraud on remote, distributed electronic systems.

Brief Description of the Figures

Figure 1 shows a schematic of an example embodiment of the present invention:

Detailed Description

For the purposes of this discussion please refer to the accompanying Figure 1.

While the embodiment described herein primarily concerns GPS data, it should be noted that any location determining system may be utilized. A fraud detection and prevention system for remote, electronic delivery of goods or services includes a multitude of subscriber terminal devices 1, which contain telecommunication links with local authorization sites 3 over various bi-directional wired 8 or wireless 9 telecommunications paths. Each terminal device contains a unique serial identification number (SIN), which is embedded in an integrated circuit within the device, as well as circuitry which receives and correlates signals from three or more Global Positioning Satellites 2 and furthermore generates global positioning system coordinates, identifying the terminal location. When a terminal device requests a transaction, it transmits the transactional data along with SIN and GPS coordinates to the authorization site along the wired 8 or wireless 0 telecom path. Authorization sites 3 are connected via high bandwidth telecommunications paths 7 to a distributed database cloud 15 having one or more database servers 5 which work in tandem to service requests from various authorization sites and which updates database records between like servers 5. Authorization sites 3 are also connected to a central database archive 6, which continuously updates its records from the distributed servers, and which redistributes its information regarding recent transactions en masse to each distributed server at certain periodic intervals of low network utilization. Only one database server 5 is required to answer a request from a given authorization site 3 for a given transaction.

Each distributed database server 5 may maintain records of up to N most recent transactions for each SIN, while the central archive contains all records for a SIN, which may be greater than N. In addition, each distributed server 5 can maintain a master list of valid SINs, periodically received from the central archive. The master list also contains a last known GPS position for each SIN. The authorization site 3 communicates the SIN and GPS information for a given transaction to a database server 5 in a validation request along a telecommunications path 7. All database servers 5, including the central archive, index their records by SIN. These servers 5 maintain transaction records including information such as SIN, transactional information such as type and price of product or service. The GPS coordinates from which the transaction was conducted, and a timestamp reflecting the server 5 received the validation request. The database servers 5 are preferably kept within 10 seconds of time synchronization. When a database server 5 receives a validation request, the server 5 verifies the SIN and retrieves the most recent transactional record which matches the SIN. If the SIN is not valid, the authorization may be rejected immediately, and a record of the request can be stored. The server 5 communicates the rejection to the authorization site via telecom path 7. If the SIN is valid, the server 5 can then compute the distance the terminal has traveled, if any, since the previous transaction. It can also compute the number of seconds which have elapsed since the last transaction. These two numbers can be used to calculate an implied groundspeed for the terminal. Threshold limits may then be established on terminal inter-transaction groundspeed which trigger an immediate warning to billing authorities and/or an automatic rejection of the transaction. Levels of distinction could also be programmed. The database server could give a warning if a fast, but possible speed was implied (if a terminal were in flight on a jet, for instance), and could give a rejection if an impossible speed was implied (if two transactions requests were registered from the same SIN simultaneously from New York and San Francisco, signaling a clear SIN cloning attempt). A SIN could also be invalidated across all database servers upon a rejection.

In a practical implementation of the system, SIN and GPS receiver circuitry are preferably installed in tamperproof IC packages, and strong encryption would be used on all transmissions in the transaction validation protocol.

Even in the case where encryption is not used, or it is broken, the cloned device must still be made to transmit false GPS coordinates which correspond to within a close proximity (as small as 9 meters) of the legitimate device, each time it is used. Otherwise, there is still the means of detection if the cloned device transmits false coordinates different from the legitimate device in close temporal association.

Example

The example concerns simultaneous transactions originating in New York and San Francisco, and is depicted in Figure 1. A subscriber who lives in San Francisco owns a terminal 1a. He is registered with the billing authority under the name John Q. Public, with his San Francisco address and phone number. A unique SIN, #5555555, was issued to him and is associated with his registration, reflecting the number hardwired into the tamperproof assembly inside his terminal device. John Q. uses his terminal without disturbance for a few months, mostly in San Francisco and the surrounding area. Then John Q. travels to New York City to visit a friend for a week, taking his terminal with him. While in New York, he uses the terminal several times, in wireless mode, to check his e-mail. Unknown to John, an individual in New York has stolen his SIN from the air and cloned John's terminal. A few days after his return to San Francisco, the thief begins using the cloned device. John wakes up one morning at 9 am and decides to check his e-mail over a dialup service in San Francisco. In connecting to his mail service, John leaves a transaction record including his SIN, GPS coordinates and time (normalized to Greenwich Mean Time) in the central database, and is soon disseminated throughout the distributed database cloud. At 12:30 pm EST, the New York-based thief calls a distant foreign country and talks to friends and family for a few hours, all to be charged to John's account. He uses his cloned terminal 1b, which also contains SIN #5555555. When the initial request for service is processed, the validation process looks up the last transaction on SIN #5555555, finding John's e-mail retrieval from San Francisco half an hour earlier, and yields an implied ground speed of about 6,000 miles per hour (3,000 miles / .5 hours), well above the impossibility threshold set up by the billing authority. The request is denied, John Q. Public's SIN is marked as invalid, and John is quickly notified he needs to register for a new SIN, before any money has been lost.

The example above makes certain simplifications for clarity, such as a cloned device in New York and the original in San Francisco, the obvious nature of the fraudulent use, and the immediate disabling of the SIN. In practice, GPS can provide a detailed resolution of cloning within a single metropolitan area, since coordinates are accurate to within 9 meters of a terminal's actual position. Another consideration is that in practice it may take several fraudulent transactions until a suitable coincidence of subscriber and thief, each trying to use the system, flags the problem. Regardless of this limitation, the system still provides a facility for detecting such fraud automatically, before a complete billing cycle has expired, reducing total losses. In addition, if fraud is suspected, a subscriber might use an active option on their terminal to continuously transmit GPS data to an authorization site in an effort to catch a thief in the act. Given the processing speed of current servers and the high communications speeds possible between computer systems, a delay of only a few seconds to check SINs against a database is achievable.

What Is Claimed Is:

1. A network system for delivering information with fraud detection and fraud prevention, comprising:

a plurality of electronic terminal devices;

a protocol for communicating over at least one telecommunications link which interconnects said devices on the network;

a coordinate locator locating each of said plurality of terminals;

at least one billing authority node connected to the network, said node communicating with said plurality of terminal devices, and said node maintaining records of terminal usage and terminal owner liability due to such usage, such that said plurality of terminal devices communicate with said at least one billing authority node using said protocol, such that said plurality of terminal devices, via said protocol, obtain approval of delivery of the information via said network to said terminal devices from said at least one billing authority and incur liability with said at least billing authority for the terminal owner, wherein the liability is recorded in at least one database connected to said at least one billing authority.

2. A method for the detection and prevention of fraud in an electronic network system, utilizing terminal location information, comprising the step of:

(a) associating in a database linked to a billing authority via a billing authority node, for at least one transaction, information identifying a transaction record.

3. The method of claim 2, wherein said transaction record is complete and includes:

i. a terminal device ID;

ii. a terminal owner;

iii. location information locating the terminal at a time corresponding to the start of the transaction;

iv. the time at which the billing authority started processing the transaction;

v. a description of the information or service involved in the transaction;

vi. the time at which the billing authority finished processing the transaction;

vii. the location coordinates at the end of the transaction;

viii. the cost of the transaction.

4. The method of claim 2, wherein said transaction record is partial and includes:

i. a terminal device ID;

ii. a terminal owner;

iii. location information at a time corresponding to the start of the transaction;

iv. the time at which the billing authority started processing the transaction;

v. a description of the information or service involved in the transaction.

5. The method of claim 3, further comprising the step of receiving from said plurality of terminal devices using said protocol:

i. terminal device ID;

ii. location information;

iii. a description of the information or service involved in the transaction;

iv. the location information at the end of the transaction.

6. The method of claim 3, further comprising the step of providing from the billing authority elements corresponding to:

i. a terminal owner;

ii. the time at which said at least one billing authority started processing the transaction;

iii. the time at which said at least one billing authority finished processing the transaction.

7. The method of claim 2, further comprising the step of determining said terminal owner from said terminal device ID by looking up an ownership record which associates a terminal owner with a terminal device ID, the status of said terminal device id, and the last reported location of the terminal device.

8. The method of claim 2, further comprising the step of determining the time at which said at least one billing authority started processing the transaction and the time at which said at least one billing authority finished processing the transaction from the local time.

9. The method of claim 3, further comprising the steps of:

a. determining items i-iv at the start of a new transaction, using said terminal device ID to search ownership records in said database to determine the validity of terminal device ID, wherein if said terminal device ID is not valid, alerting said billing authority and storing a record containing information items i-v in a list of denied transactions.

10. The method of claim 2, further comprising the step of using item i to search transaction records in said database for the most recent previously existing

transaction record which matches the terminal device ID.

11. The method of claim 2, further comprising the step of finding matching transaction records, comparing the time and location of the previous record with the time and location of the new record, and imputing an implied ground-speed for the terminal device, between current and previous transaction.

12. The method of claim 11, further comprising the step of comparing the implied ground speed with a threshold limit set by the billing authority, approving the transaction if the implied ground speed is at or below the threshold, and denying the transaction authorization if the ground speed is above the threshold.

13. The method of claim 4, further comprising the step of alerting the billing authority, storing a record of information items i-iv in a list of denied transactions.

14. A network system with fraud detection and fraud prevention, comprising:

a plurality of electronic terminal devices;

means to deliver information to the terminal user via the network;

means to incur liability to the registered terminal owner in exchange for the provision of the information;

a protocol for communicating over at least one telecommunications link which interconnects said plurality of devices on the network;

at least one billing authority node connected to said network, communicating with said plurality of terminal devices, said node maintaining records of terminal usage and terminal owner liability due to such usage, such that said plurality of terminal devices communicate with said at least one billing authority node via telecommunications links which connect the terminals with billing authority nodes;

wherein said billing authority analyzes the telecommunications link to said terminal to provide coordinates describing the location of said terminal device;

such that said plurality of terminal devices use said protocol to obtain approval of delivery of information via said network to said plurality of terminal devices from said at least one billing authority and incur liability with said at least one billing authority for the terminal owner, wherein the liability is recorded in at least one database connected to said at least one billing authority.

15. A network system with fraud detection and fraud prevention, comprising:

a plurality of electronic terminal devices;

means to deliver information to the terminal user via the network, means to incur liability to a registered terminal owner in exchange for the provision of the goods or services;

a protocol for communicating over at least one telecommunications link connecting the devices on the network;

a coordinate locator locating said terminal;

at least one billing authority node connected to said network, said at least one node communicating with said plurality of terminal devices, said node maintaining records of terminal usage and terminal owner liability;

such that said plurality of terminal devices communicate with said at least one billing authority node via telecommunications links which connect the terminals with billing authority nodes;

wherein said at least one billing authority analyzes the telecommunications link to one of said plurality of terminal devices to provide coordinates describing the location of said one of said terminal devices;

and such that said plurality of terminal devices use said protocol to obtain approval of delivery of information via said network to said plurality of terminal devices from said at least one billing authority.

16. The method of claim 2, further comprising the step of combining a threshold ground speed limit with a predetermined region of valid coordinates, and pre-programmed into the database, such that said region is associated with the ownership record for the device ID of the owner and said region is used to screen validation, such that the billing authority rejects any transactions outside the region regardless of groundspeed, and allows any transactions within the region which do not exceed the groundspeed threshold.

17. The method of claim 2, further comprising the step of incorporating a user controlled "active" locating option into a terminal device such that it continuously broadcasts its location to a billing authority in an attempt to increase the probability of detection of fraudulent transactions by a cloned device, such that as each transmission is received, the location is noted in the SIN master list as the last location coordinates.

18. The method of claim 2, wherein said terminal device ID is supplemented by ID codes other than the device ID to isolate occurrences of fraud using

misappropriated account numbers from non-cloned computing devices.

19. The method of claims 2, further comprising the step of using encryption techniques to encode the transmission of sensitive ID codes, location information, and time stamp data from one of said plurality of terminal devices to said billing authority.

20. The method of claim 9, further comprising the step of invalidating the terminal identification number.

1/1

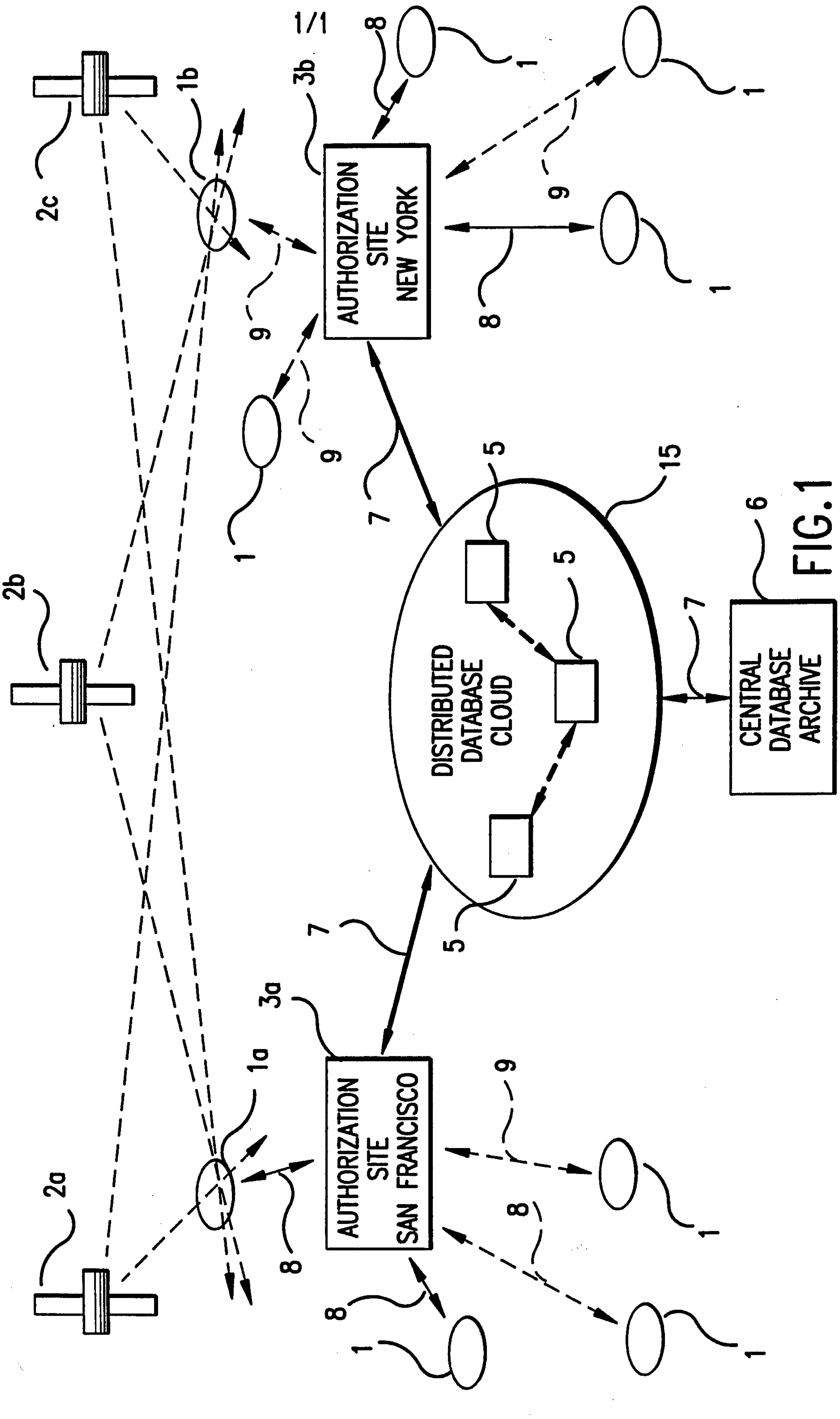

2c
2b
2a
1b
1a
3b
3a
AUTHORIZATION SITE NEW YORK
AUTHORIZATION SITE SAN FRANCISCO
DISTRIBUTED DATABASE CLOUD
CENTRAL DATABASE ARCHIVE
1
5
6
7
8
9
15

FIG.1

INTERNATIONAL SEARCH REPORT

Ii. ıational application No.
PCT/US96/10096

A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) :H04Q 7/00
US CL : 340/825.33
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 340/825.33, 825.35, 825.34, 825.31, 825.36, 825.49; 379/59, 60, 62, 91, 95; 455/54.1, 33.1; 364/449; 380/23, 49; 342/357

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

APS search terms: gps, global, position, geographic, location, transaction, database, time, fraud, authenticate

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X ---- Y	US, A, 5,345,595, (JOHNSON ET AL.) 06 September 1994, abstract, figures 1b, 2, and 8, column 5 line 4 - column 9 line10, column 12 line 52 - column 16 line 36 and column 31 line 37-47.	1-15, 20 ------------ 16-19
X ---- Y	US, A, 5,335,265 (COOPER ET AL.) 02 August 1994, abstract, figures 1-5, column 1 line 45 - column 2 line 36, column 2 line 48 - column 3 line 60, column 4 line 20 - column 10 line 46.	1-2, 4, 7-8, 10-15, 18 --------------- 3, 5-6, 9, 16-17, 19-20
Y	US, A, 5,235,633 (DENNISON ET AL) 10 August 1993, abstract, column 3 line 31 - column 4 line 13 and column 5 line 30 - column 6 line 12.	1-20

☒ Further documents are listed in the continuation of Box C. □ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

22 SEPTEMBER 1996

Date of mailing of the international search report

31 OCT 1996

Name and mailing address of the ISA/US
Commissioner of Patents and Trademarks
Box PCT
Washington, D.C. 20231
Facsimile No. (703) 305-3230

Authorized officer for Diane
EDWIN C. HOLLOWAY, III
Telephone No. (703) 305-4900

INTERNATIONAL SEARCH REPORT

I .national application No.
PCT/US96/10096

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y,E	US, A, 5,535,431 (GRUBE ET AL.) 09 July 1996, abstract, column 2 line 60 - column 3 line 55.	1-20
Y	US, A, 5,365,451 (WANG ET AL) 5,365,451 15 November 1994, abstract figures 7 and 9-11, column 1 line 1 - column 2 line 13, column 3 lines 28-61 and column 7 line 46 - column 9 line 13.	1-20
Y	US, A, 5,335,278 (MATCHETT ET AL.) 02 August 1994, abstract and column 9 line 56 - column 11 line 37.	18-19