US 20030093690A1

(19) United States

(12) Patent Application Publication (10) Pub. No.: US 2003/0093690 A1

Kemper (43) Pub. Date: May 15, 2003

(54) COMPUTER SECURITY WITH LOCAL AND REMOTE AUTHENTICATION

(76) Inventor: **Stefan Kemper**, Boise, ID (US)

Correspondence Address:
HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400 (US)

(21) Appl. No.: **10/003,138**

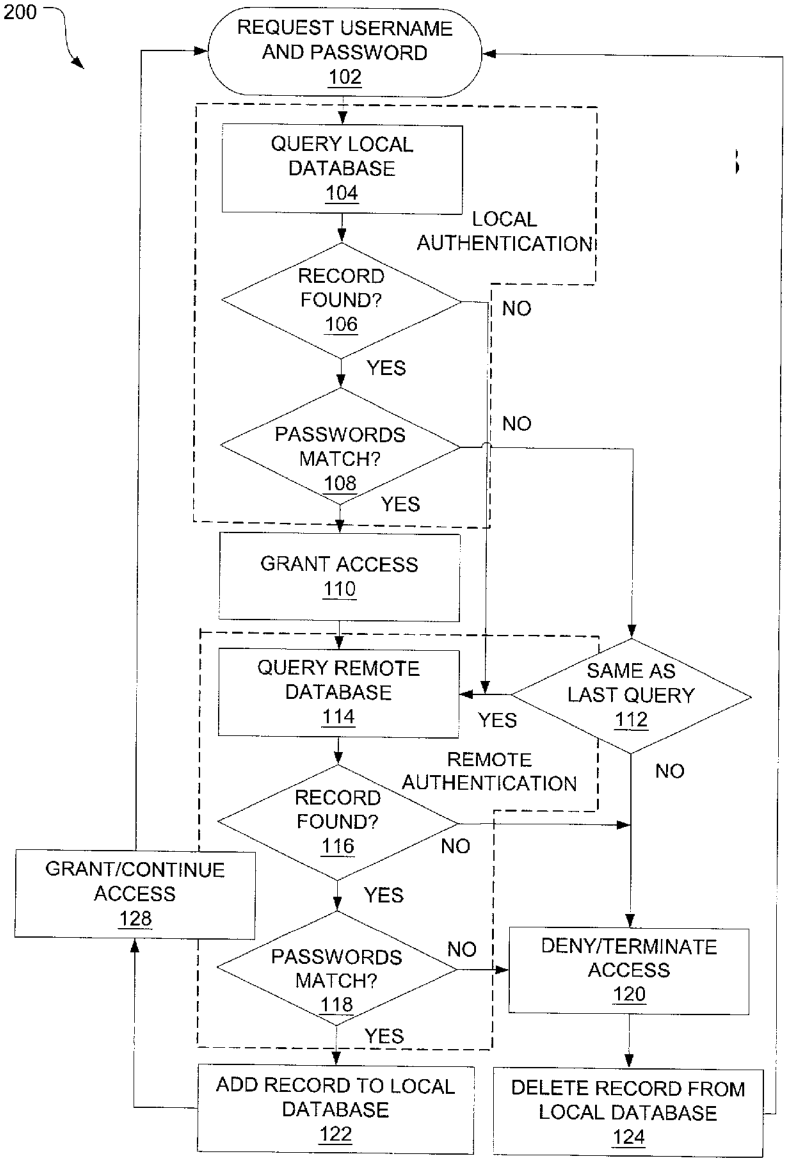
(22) Filed: **Nov. 15, 2001**

Publication Classification

(51) Int. Cl.[7] **H04L 9/00**
(52) U.S. Cl. **713/201**

(57) ABSTRACT

A secure computer system including a client having a client database for locally-authenticating a user; and a server, in communication with the client, having a server database for remotely-authenticating the user in response to a request from the client. The system also provides updating of the client database according to results of the local and remote authentication.



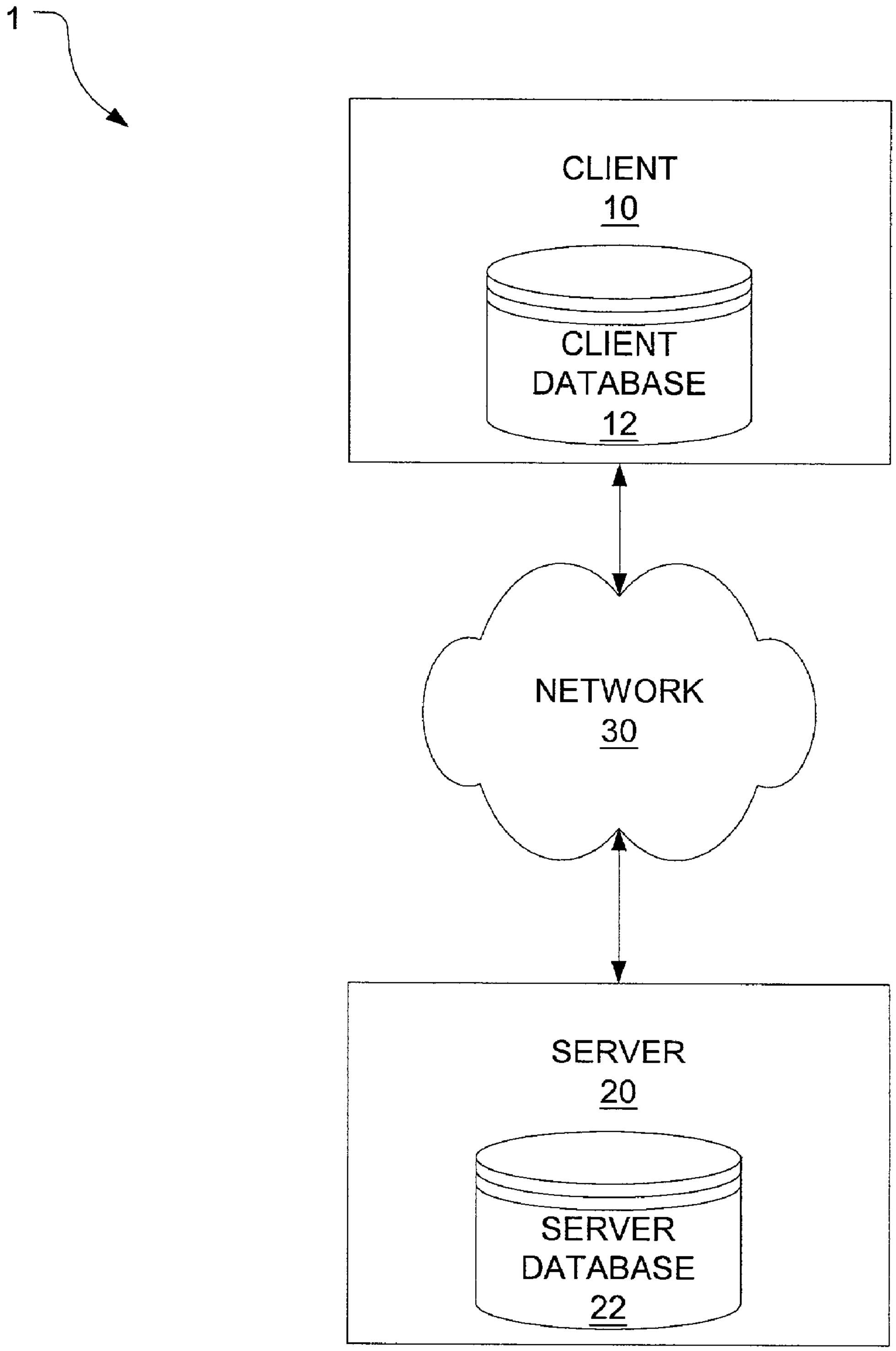

1
CLIENT
10
CLIENT
DATABASE
12
NETWORK
30
SERVER
20
SERVER
DATABASE
22

FIG. 1

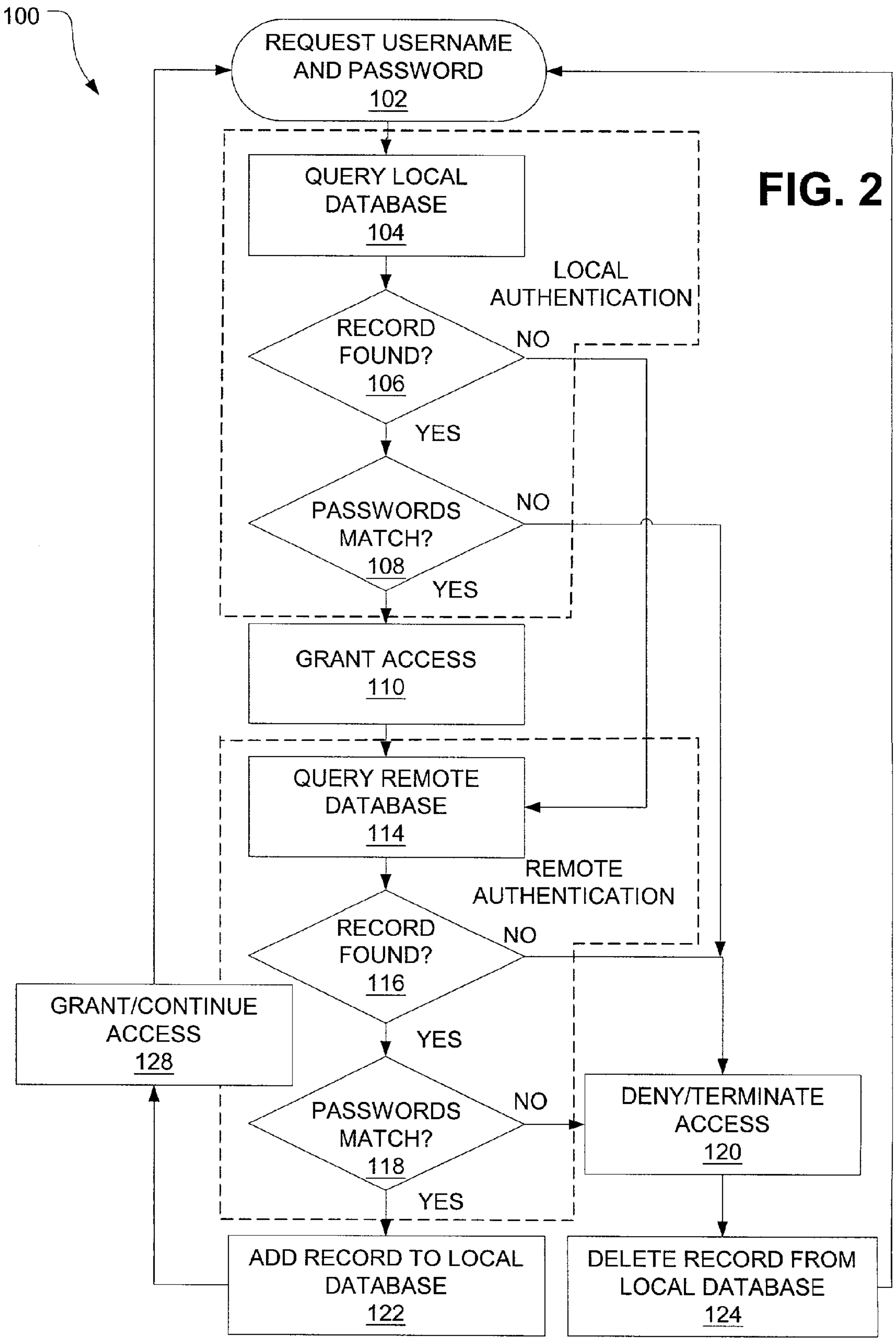

100
REQUEST USERNAME AND PASSWORD 102
QUERY LOCAL DATABASE 104
LOCAL AUTHENTICATION
RECORD FOUND? 106
NO
YES
PASSWORDS MATCH? 108
NO
YES
GRANT ACCESS 110
QUERY REMOTE DATABASE 114
REMOTE AUTHENTICATION
RECORD FOUND? 116
NO
YES
GRANT/CONTINUE ACCESS 128
PASSWORDS MATCH? 118
NO
YES
DENY/TERMINATE ACCESS 120
ADD RECORD TO LOCAL DATABASE 122
DELETE RECORD FROM LOCAL DATABASE 124

FIG. 2

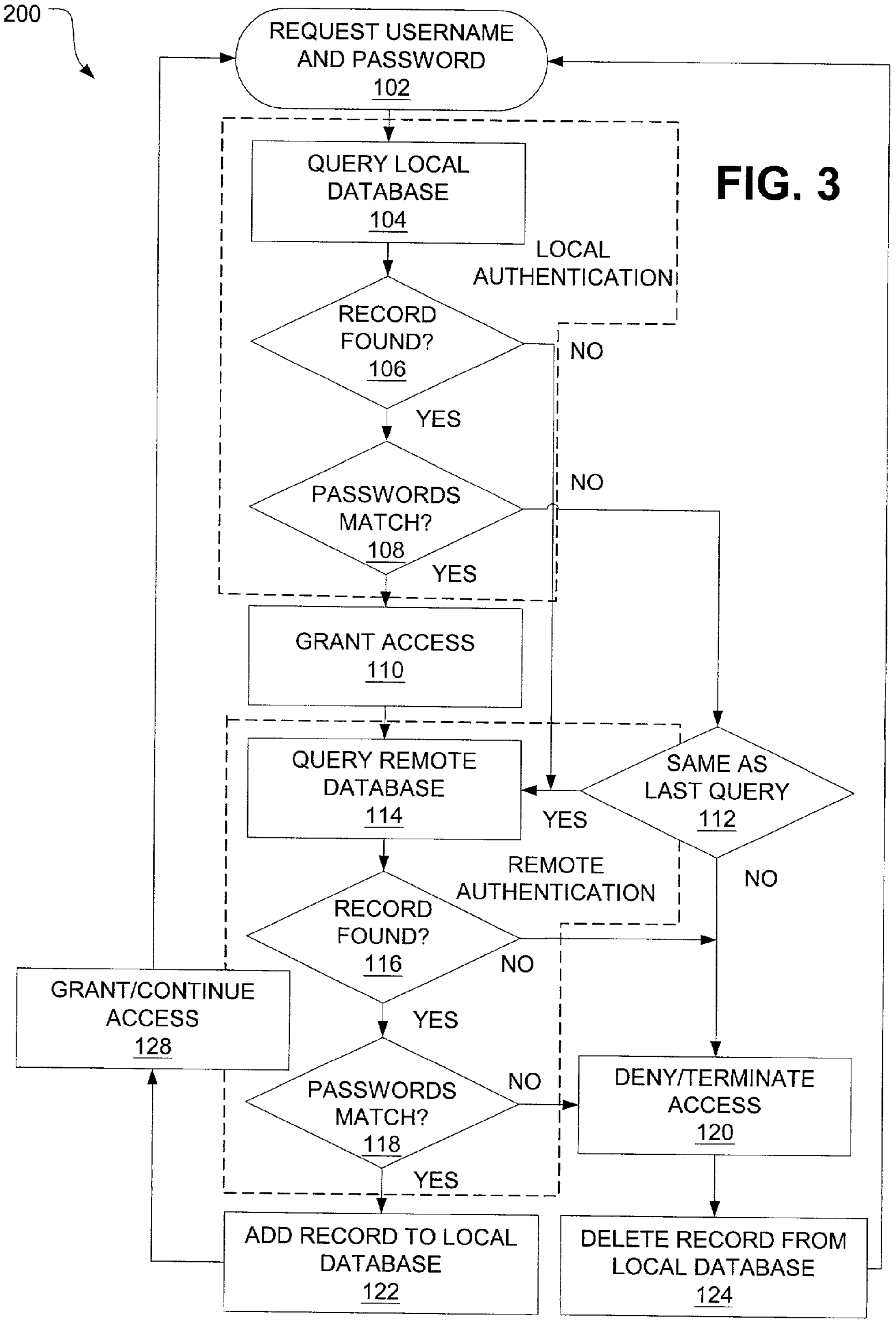

200
REQUEST USERNAME AND PASSWORD 102
QUERY LOCAL DATABASE 104
LOCAL AUTHENTICATION
RECORD FOUND? 106
NO
YES
PASSWORDS MATCH? 108
NO
YES
GRANT ACCESS 110
QUERY REMOTE DATABASE 114
SAME AS LAST QUERY 112
YES
NO
REMOTE AUTHENTICATION
RECORD FOUND? 116
NO
YES
GRANT/CONTINUE ACCESS 128
PASSWORDS MATCH? 118
NO
YES
DENY/TERMINATE ACCESS 120
ADD RECORD TO LOCAL DATABASE 122
DELETE RECORD FROM LOCAL DATABASE 124

FIG. 3

COMPUTER SECURITY WITH LOCAL AND REMOTE AUTHENTICATION

TECHNICAL FIELD

[0001] The subject matter disclosed here generally relates to security support for electrical computers and digital processing systems, and, more particularly, to an apparatus, method, and logic for authentication and authorization of a user.

BACKGROUND

[0002] Authentication and authorization are important aspects of any security system, including computer security systems. "Authentication" refers to the verification of the identity of a person or process before they perform other system actions. In a communication system, authentication may involve simply verifying that a message comes from its stated source. For example, a bank might compare the signature on a hand-written check to a sample signature on file. Like signatures, however, many other forms of personal identification can also be forged. Consequently, so-called "strong authentication" uses a combination of items belonging to at least two of the following three categories: 1) personal knowledge (such as a password or personal identification number); 2) personal possessions (such a cardkey or other physical token); and 3) personal characteristics (such as a handwriting sample, voiceprint, fingerprint, or retina scan).

[0003] In general terms, "authorization" is the process of enforcing policies for authenticated entities, such as policies for determining what types of activities, resources, or services may be used. Typically, once an entity has been authenticated, the authorization process will determine whether that entity has the authority to issue certain commands. For example, in the check-writing scenario described above, a bank might confirm the availability of funds in the payer's account before following the instruction on the check to transfer funds to the payee. Similarly, in an electronic computer system, the authorization process may automatically provide an authenticated individual (who is logged on with the correct username and password) with the authority to issue any command. In fact, "access control" is the primary means for enforcing authorization policies by granting, denying, and/or terminating access to an unauthorized process or device.

[0004] Authentication, authorization, and accounting ("AAA") is a term that is sometimes used to describe a general framework for intelligently controlling access to computer resources, enforcing policies, auditing usage, and providing the information necessary to manage those resources. Various Requests for Comments ("RFC's) of the Internet Engineering Task Force ("IETF") discuss such a framework and are incorporated by reference here, including RFC 2903 entitled "Generic AAA Architecture," RFC 2904 entitled "AAA Authorization Framework," RFC 2905 entitled "AAA Authorization Application Examples," and RFC 2906 entitled "AAA Authorization Requirements." In general terms, these documents describe a system where an "AAA server" is used to provide authentication, authorization, and/or accounting services in response to a user's request. The AAA server inspects the contents of the request, determines what authorization is requested, retrieves policy rules from a repository, and then either grants the requested access or passes along the request to another AAA server.

[0005] One standard protocol by which many devices and applications communicate with an AAA server is the Remote Authentication Dial-In User Service ("RADIUS") described in Request for Comment ("RFC") 2865, and others, of the Internet Engineering Task Force ("IETF") which is also incorporated by reference here. RADIUS is a client/server protocol that enables remote access servers to communicate with a central server in order to authenticate dial-in users and authorize their access to a requested system or service. RADIUS allows an organization to maintain user profiles in a central database that all remote servers can share. It thus provides for improved security by allowing computer resource owners to administer their authorization policies at a single network point.

[0006] RADIUS and other such security protocols that rely on centralized databases for authorization can be quite slow, especially when implemented with low capacity communications networks. For example, in many prior art systems, authentication requires digitally signing the request, as well as the exchange of information called "credentials" between the requester and the server. The authentication process can therefore impose significant overhead on the operation of distributed computer systems, especially when the number of requests transmitted is high.

[0007] U.S. Pat. No. 5,235,642 to Wobber et al. discloses an apparatus and method for making such access control systems more efficient by caching authentication credentials. A computer at each node of a distributed system has a trusted computing base that includes an authentication agent for authenticating requests received from principals at other nodes in the system. Requests are transmitted to the servers as messages that include a first identifier (called an Auth ID) provided by the requester and a second identifier provided (called the subchannel value) by the authentication agent of the requester node.

[0008] Each server process has an associated local cache that identifies requesters whose previous request messages have been authenticated. When a request is received, the server checks the request's first and second identifiers against the entries in its local cache. If there is a match, then the request is known to be authentic, without having to obtain authentication credentials from the requester's node.

[0009] If the identifier in a request message does not match any of the entries in the server's local cache, then the server node's authentication agent is called to obtain authentication credentials from the requester's node to authenticate the request message. Upon receiving the required credentials from the requester node's authentication agent, the principal identifier of the requester and the received credentials are stored in a local cache by the server node's authentication agent. The server process also stores a record in its local cache indicating that request messages from the specified requester are known to be authentic, thereby expediting the process of authenticating received requests.

[0010] Although the Wobber et al. server cache may help minimize server loads, it does not address the problem of communication load and/or lag times between the client requester and the server.

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.

WHAT WILL YOU BUILD? | **sales@docketalarm.com** | **1-866-77-FASTCASE**

fastcase®
Smarter legal research.