



(19)
Bundesrepublik Deutschland
Deutsches Patent- und Markenamt

(10) **DE 10 2005 015 919 B4 2008.10.16**

(12)

Patentschrift

(21) Aktenzeichen: **10 2005 015 919.2**
(22) Anmeldetag: **06.04.2005**
(43) Offenlegungstag: **27.10.2005**
(45) Veröffentlichungstag
der Patenterteilung: **16.10.2008**

(51) Int Cl.⁸: **G06F 12/14 (2006.01)**
G06F 21/00 (2006.01)
G06F 21/20 (2006.01)
G06F 15/163 (2006.01)

Innerhalb von drei Monaten nach Veröffentlichung der Patenterteilung kann nach § 59 Patentgesetz gegen das Patent Einspruch erhoben werden. Der Einspruch ist schriftlich zu erklären und zu begründen. Innerhalb der Einspruchsfrist ist eine Einspruchsgebühr in Höhe von 200 Euro zu entrichten (§ 6 Patentkostengesetz in Verbindung mit der Anlage zu § 2 Abs. 1 Patentkostengesetz).

(66) Innere Priorität:
10 2004 018 129.2 08.04.2004

(73) Patentinhaber:
symmedia GmbH, 33602 Bielefeld, DE

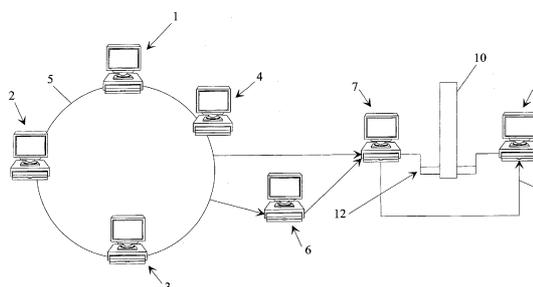
(74) Vertreter:
Eikel & Partner GbR, 32760 Detmold

(72) Erfinder:
Baumann, Michael, 33602 Bielefeld, DE

(56) Für die Beurteilung der Patentfähigkeit in Betracht
gezogene Druckschriften:
US2002/00 49 912 A1
US 61 61 182

(54) Bezeichnung: **Zugriffsverfahren auf Device Server eines Maschinennetzwerkes**

(57) Hauptanspruch: Verfahren für die Regelung eines elektronischen Zugriffs auf mit Device Servern versehene Vorrichtungen wie Werkzeugmaschinen oder dergleichen, die in einem einen LookUp Server aufweisenden Netzwerk eingebunden sind, dadurch gekennzeichnet,
– dass für eine Fernwartung von dem Device Server (1–4) einer Vorrichtung eine Serviceanforderung ergeht,
– dass von dem LookUp Server (6) auf einem zentralen, in das Internet (10) eingebundenen Relay Server (7) ein Service-Ticket angelegt wird,
– dass der Relay Server (7) auf eine Serviceanforderung eine Nachricht generiert und an eine vorbestimmten Gruppe von Serviceleistenden (9) absetzt und
– dass der Gruppe über das Service-Ticket ein unmittelbarer Zugriff auf den Device Server (1–4) der Vorrichtung gestattet wird.



Beschreibung

[0001] Die Erfindung betrifft ein Verfahren für die Regelung eines elektronischen Zugriffs auf mit Device Servern versehene Vorrichtungen wie Werkzeugmaschinen, Produktionsmaschinen oder dergleichen Einrichtungen und Geräte, die in einem einen LookUP Server aufweisenden Netzwerk eingebunden sind.

[0002] Computernetzwerke sind in vielfältigen Ausführungen bekannt und bewährt. Zumeist weisen derartige Netzwerke einen Server für administrative Zwecke auf, der auch die Kommunikation der in das Netzwerk eingebundenen Clients regelt. Aus der US 6,161,182 ist ein geschlossenes Netzwerk bekannt, bei dem ein Server den Zugriff von Clients auf fernsteuerbare Vorrichtungen regelt. Will bei dem dort offenbarten Verfahren ein Client auf eine fernsteuerbare Vorrichtung zugreifen, erhält der Client von der Vorrichtung eine Aufforderung, sich bei dem Server anzumelden, um die Erlaubnis für einen Zugriff zu erhalten. Der Server fragt daraufhin die Berechtigung des Clients in Form einer Identifizierung ab. Erfolgt, sofern der Client für einen Zugriff auf die Vorrichtung berechtigt ist, eine positive Identifizierung durch den Server, erhält der Client eine Zugangsberechtigung zu der Vorrichtung, die von der Vorrichtung für einen Zugriff akzeptiert wird. Nach Beendigung des Zugriffs auf die Vorrichtung meldet sich der Client bei dem Server ab, der dann letztlich dem Client die Beendigung des Zugriffs noch bestätigt.

[0003] Bei einem Netzwerk, bei dem mittels Device Servern Vorrichtungen, bspw. Werkzeugmaschinen oder dergleichen eingebunden sind, verfügen diese über eine elektronische Signatur, vergleichbar einem digitalen Typenschild, so dass unterschiedlichste Geräte innerhalb eines solchen Local Area Networks mittels eines LookUP-Dienstes eines LookUP Servers erkannt werden können.

[0004] Für eine Fernwartung kann ein Device Server beispielsweise mittels eines diesem zugeordneten Modem mit einem Rechner eines Serviceleistenden für eine Fernwartung kommunizieren. Wenn auch eine derartige Verbindung für Stand-Alone-Maschinen vergleichsweise sicher ist, weist ein Modemzugriff für vernetzte Maschinen nicht unerhebliche Risiken auf. Daher erfolgt der Zugriff auf die Vorrichtungen wie Werkzeugmaschinen oder dergleichen bei einer Fernwartung regelmäßig über den den Zugriff verwaltenden LookUP-Server. Dieser ist dazu mit einer betreiberspezifischen Netzwerkinfrastruktur versehen, insbesondere mit Firewall-Funktionalitäten.

[0005] Zwar lassen sich durch das Konzept Instandhaltungs- und Servicenetzwerke vergleichsweise einfach einrichten und administrieren, auch wenn unterschiedlichste Vorrichtungen verschiedener Hersteller

in komplexen Datennetzen eingebunden sind, jedoch genügen die wie aus der US 6,161,182 bekannten Verfahren bei der Gestaltung von externen Zugriffsszenarien kaum den hohen Sicherheitsansprüchen, die derartige Netze regelmäßig erfüllen müssen.

[0006] Vor diesem technischen Hintergrund macht die Erfindung es sich zur Aufgabe, ein Verfahren für die Regelung eines elektronischen Zugriffs auf mit Device Servern versehene Vorrichtungen wie Werkzeugmaschinen oder dergleichen, die in einem einen LookUP Server aufweisenden Netzwerk eingebunden sind, zur Verfügung zu stellen, das auch höchsten Sicherheitsanforderungen genügt.

[0007] Zur Lösung dieser technischen Problematik wird gemäß des Anspruchs 1 darauf abgestellt, dass für eine Fernwartung von dem Device Server einer Vorrichtung eine Serviceanforderung ergeht, dass von dem LookUP Server auf einem zentralen, in das Internet eingebundenen Relay Server ein Service-Ticket angelegt wird, dass der Relay Server auf eine Serviceanforderung eine Nachricht generiert und an eine vorbestimmten Gruppe von Serviceleistenden absetzt und dass der Gruppe über das Service-Ticket ein unmittelbarer Zugriff auf den Device Server der Vorrichtung gestattet wird.

[0008] Aufgrund dieser Maßnahmen erfolgt eine Kommunikation über das Internet bei einer Fernwartung zwischen einem Device Server, gegebenenfalls auch einer Gruppe von gleichartigen Device Servern mit einem Rechner eines Serviceleistenden vorzugsweise nicht unter Einbeziehung des LookUP Servers. Vielmehr kann dieser von der Kommunikation vollständig abgekoppelt werden. Infolge dessen kann der Zugriff des Serviceleistenden bei einer Fernwartung auf den Device Server unmittelbar erfolgen. Es ist jedoch der Zugang über das Internet für die Fernwartung nur dann überhaupt möglich, wenn das Service-Ticket von dem Relay Server erstellt wurde und das Service-Ticket ein entsprechendes Portal zur Verfügung stellt. Dieses Portal kann auch nur zeitlich beschränkt zur Verfügung gestellt werden.

[0009] Zweckmäßigerweise wird ein Serviceticket nur auf eine Serviceanforderung aus dem Netzwerk erstellt. Die hierzu nötige Kommunikation kann unmittelbar zwischen den Device Servern und dem Relay Server erfolgen oder über den LookUP Server, in jedem Fall nur gleichsam von innen nach außen.

[0010] Hierdurch wird der sichere Zugriff von außen durch ein bestehendes Firewall-Konzept gewährleistet, das im Grunde keine Verbindungen von außen nach innen in das Netzwerk akzeptiert. Es ist damit eine Zurückverbindung nur über die ausgehende Verbindung möglich (Reverse Proxy).

[0011] Dies bietet weiter den Vorteil, dass eine sol-

che Serviceanforderung unmittelbar von dem einer Vorrichtung zugeordneten Device Server, bspw. dem einer Werkzeugmaschine oder dergleichen zugeordneten, erfolgen kann, wenn bspw. ein Bediener der Vorrichtung externe Hilfe benötigt. Alternativ besteht die Möglichkeit, die Serviceanforderung über den LookUP Server auszulösen. Insbesondere dann kann es sich auch um eine regelmäßige Fernwartung handeln, die dann auch keiner manuellen Serviceanforderung bedarf.

[0012] In einer bevorzugten Ausgestaltung des Verfahrens nach der Erfindung ist weiter vorgesehen, dass der Relay Server auf eine Serviceanforderung aus dem Netzwerk eine Nachricht generiert und an die Gruppe der Serviceleistenden absetzt, wobei hier insbesondere an elektronische Nachrichten gedacht ist, vorzugsweise in Form einer E-Mail und/oder einer SMS, die der Relay Server selbst auch unmittelbar absetzen kann.

[0013] Grundsätzlich kann aber auch bspw. ein Fax generiert und per Modem übertragen werden.

[0014] Diese Nachricht enthält den Zugang für das nur für eine spezielle Serviceanforderung erstellte Service-Ticket, bspw. in Form einer Internetadresse. Daneben kann die Nachricht technische Daten noch enthalten, bspw. welche Vorrichtung ferngewartet werden soll, die Adresse des zugehörigen Device Servers in dem Netzwerk, Angaben eines Schadens oder dergleichen mehr. Insbesondere die sicherheitstechnisch relevante Daten, wie die Adressen, können aber auch in dem Service-Ticket hinterlegt sein und werden erst bei einem berechtigten Zugriff zur Verfügung gestellt.

[0015] Als zweckmäßig hat es sich erwiesen, wenn der Relay Server die Serviceanforderungen listet. Es ist dann ein Vergleich zwischen tatsächlichen Zugriffen auf das Netz und den tatsächlich angeforderten ermöglicht, so dass unberechtigte Zugriffe erkannt werden können.

[0016] Erfolgt nach der Benachrichtigung eines Serviceleistenden über den Bedarf einer Fernwartung ein Zugriff, wird auch der Zugriff des Serviceleistenden von den Relay Server zunächst auf eine Berechtigung überprüft werden. Bei einem Fehlen von beispielsweise Sicherheitsprotokollen, Passwörtern oder dergleichen wird eine Berechtigung nicht anerkannt und ein Zugriff auf das Netzwerk verwehrt.

[0017] Die Sicherheit der Kommunikation kann weiter durch die Maßnahmen erhöht werden, dass eine verschlüsselte Verbindung zwischen den LookUP Server bzw. dem Device Server und dem Relay Server aufgebaut wird.

[0018] Als eine weitere Sicherheitsmaßnahme ist

vorgesehen, dass die Verbindung mit Abschluss des Services und/oder nach einer vorgebbaren Zeit von dem LookUP Server unterbrochen wird.

[0019] Für eine Vereinfachung der administrativen Verwaltung des Netzwerkes kann es zweckmäßig sein, dass eine elektronische Signatur eines Device Servers einer Vorrichtung wie einer Werkzeugmaschine oder dergleichen eine Angabe enthält, die dem LookUP Server und/oder dem Relay Server eine Freischaltung für einen Zugriff für eine Fernwartung erlaubt.

[0020] Device Server, die keiner Fernwartung bedürfen, sind damit einem unzulässigen Zugriff sicher entzogen, da für diese Server keine Freischaltung erfolgt, diese dem Relay Server gleichsam nicht bekannt sind, wohl aber dem LookUP Server.

[0021] Dieses Verfahren nach der Erfindung wird anhand der Zeichnung näher erläutert, in der schematisch die Kommunikationswege für eine Fernwartung dargestellt sind. In der Zeichnung zeigt:

[0022] [Fig. 1](#): die Kommunikationswege bei einer Serviceanforderung und

[0023] [Fig. 2](#): die Kommunikationswege bei einer Fernwartung.

[0024] In [Fig. 1](#) sind beispielhaft vier Device Server **1** bis **4** in einem Netzwerk **5** eingebunden.

[0025] Die Device Server **1** bis **4** können nahezu beliebigen Vorrichtungen zugeordnet sein, auch solchen unterschiedlichster Hersteller, wozu jeder Device Server **1** bis **4** mit einer die zugeordnete Vorrichtung charakterisierende elektronische Signatur versehen ist.

[0026] Verwaltet wird das Netzwerk **5** von einem LookUP Server **6**, der mit einem Suchdienst versehen das Netzwerk **5** nach den Device Servern **1** bis **4** absuchen, das Netzwerk scannen kann. Anhand der elektronischen Signaturen werden dabei die Device Server **1** bis **4** erkannt und verwaltet werden.

[0027] Bedarf es bei einer der den Device Servern **1** bis **4** zugeordneten Vorrichtungen externer Hilfe, einer Fernwartung, kann direkt auf einem der Device Server **1** bis **4** beispielsweise von einem Benutzer, alternativ von einem Administrator über den LookUP Server **6**, eine Serviceanforderung ausgelöst werden, die erfindungsgemäß einem Relay Server **7** gemäß den Pfeilen in [Fig. 1](#) zugeht.

[0028] Der Relay Server **7** ist in das Internet **10** eingebunden, erlaubt jedoch im Regelfall keinen Zugriff aus diesem auf das Netzwerk **5**.

[0029] Auf eine Serviceanforderung aus dem Netzwerk **5** wird der Relay Server **7** eine Nachricht generieren, bevorzugt eine elektronische, beispielsweise eine E-Mail oder eine SMS, ggfls. aber auch ein Fax, wenn der Relay Server **7** mit einem Modem beispielsweise versehen ist, und er wird diese Nachricht gemäß Pfeil **8** an eine Gruppe von Serviceleistenden **9** absetzen.

[0030] Auf die Serviceanforderung aus dem Netz **5** wird der Relay Server **7** weiter ein Service-Ticket anlegen, über das der bzw. die Serviceleistenden **9** auf eine oder eine Gruppe von Vorrichtungen für eine Fernwartung zugreifen kann, die den Device Servern **1 bis 4** zugeordnet ist bzw. sind.

[0031] Für einen Zugriff bei einer Fernwartung auf eine der den Device Servern **1 bis 4** zugeordnete Vorrichtung erhalten die Serviceleistenden **9** mit der Nachricht gemäß Pfeil **8** den Zugang zu dem Service-Ticket, beispielsweise in Form einer Internetadresse. Speziell für diese eine Serviceanforderung öffnet der Device Server ein Portal **11**, vgl. [Fig. 2](#), gegebenenfalls zeitlich limitiert und/oder nur zu bestimmten Zeiten. Über das Portal bzw. das Service-Ticket können die Serviceleistenden **9** damit einen Zugriff auf eine oder eine Gruppe der den Device Servern **1 bis 4** zugeordneten Vorrichtungen nehmen. Dieser Zugriff kann über den LookUP **6** erfolgen, wird jedoch in der Regel unmittelbar von dem Relay Server **7** auf den entsprechenden Device Server **1 bis 4** unmittelbar erfolgen.

[0032] Wenn der Zugriff der Serviceleistenden **9** über das Internet **10** und das Portal **11** auf den Relay Server **7** erfolgt, wird von diesem die Berechtigung des Zugriffs zunächst überprüft. Solches kann in an sich üblicher Weise durch Passworte geschehen, die beispielsweise auch mit der Nachricht gemäß Pfeil **8** oder anderweitig übermittelt worden sind. Insbesondere bedarf es jedoch einer Übereinstimmung mit dem Zugriff und der von dem Relay Server gelisteten Serviceanforderung, beispielsweise auf Übereinstimmung der Zuordnung des Serviceleistenden **9** mit der einem der Device Servern **1 bis 4** zugeordneten Vorrichtung oder dergleichen mehr. Insbesondere wird durch eine Listung der Serviceanforderungen auch ein unberechtigter Zugriff sicher erkannt.

[0033] Ist die Fernwartung korrekt beendet, wird von dem Relay Server **7** das Portal **11** wieder geschlossen und der gesamte Vorgang protokolliert. Eine hohe Sicherheitsschwelle ist damit gegeben. Alternativ kann von dem LookUP Server **6** und/oder dem Relay Server **7** nach einer vorgebbaren Zeit die Verbindung mit dem Internet **10** unterbrochen werden. Dabei erfolgt die Kommunikation insbesondere zwischen dem LookUP Server **6** und dem Relay Server **7** bevorzugt verschlüsselt, wie auch die Verbindung zwischen dem Relay Server **7** und den Device Ser-

vern **1 bis 4** der fernzuwartenden Vorrichtungen.

[0034] Neben der erläuterten Serviceanforderung und der darauf folgenden Fernwartung kann der Relay Server natürlich auch weitere Fernwartungen oder Internetdienste über Portale **12** verwalten.

Patentansprüche

1. Verfahren für die Regelung eines elektronischen Zugriffs auf mit Device Servern versehene Vorrichtungen wie Werkzeugmaschinen oder dergleichen, die in einem einen LookUP Server aufweisenden Netzwerk eingebunden sind, **dadurch gekennzeichnet**,

- dass für eine Fernwartung von dem Device Server (**1–4**) einer Vorrichtung eine Serviceanforderung ergeht,
- dass von dem LookUP Server (**6**) auf einem zentralen, in das Internet (**10**) eingebundenen Relay Server (**7**) ein Service-Ticket angelegt wird,
- dass der Relay Server (**7**) auf eine Serviceanforderung eine Nachricht generiert und an eine vorbestimmten Gruppe von Serviceleistenden (**9**) absetzt und
- dass der Gruppe über das Service-Ticket ein unmittelbarer Zugriff auf den Device Server (**1–4**) der Vorrichtung gestattet wird.

2. Verfahren nach einem oder mehreren der vorangehenden Ansprüche, dadurch gekennzeichnet, dass nur über eine ausgehende Verbindung eine Zurückverbindung möglich ist.

3. Verfahren nach einem oder mehreren der vorangehenden Ansprüche, dadurch gekennzeichnet, dass die Nachricht eine elektronische Nachricht ist.

4. Verfahren nach einem oder mehreren der vorangehenden Ansprüche, dadurch gekennzeichnet, dass die Nachricht den Zugang für das Service-Ticket enthält.

5. Verfahren nach einem oder mehreren der vorangehenden Ansprüche, dadurch gekennzeichnet, dass für den Zugang für das Service-Ticket eine Internetadresse (URL) übermittelt wird.

6. Verfahren nach einem oder mehreren der vorangehenden Ansprüche, dadurch gekennzeichnet, dass der Relay Server (**7**) die Serviceanforderungen listet.

7. Verfahren nach einem oder mehreren der vorangehenden Ansprüche, dadurch gekennzeichnet, dass die Berechtigung des Zugriffs eines Serviceleistenden (**9**) von dem Relay Server (**7**) überprüft wird.

8. Verfahren nach einem oder mehreren der vorangehenden Ansprüche, gekennzeichnet durch eine

verschlüsselte Verbindung zwischen dem LookUp Server (6) und dem Relay Server (7).

9. Verfahren nach einem oder mehreren der vorangehenden Ansprüche, dadurch gekennzeichnet, dass die Verbindung mit Abschluß der Fernwartung und/oder nach einer vorgebbaren Zeit von dem LookUp Server (6) und/oder dem Relay Server (7) unterbrochen wird.

10. Verfahren nach einem oder mehreren der vorangehenden Ansprüche, dadurch gekennzeichnet, dass eine elektronische Signatur eines Device Servers (1-4) einer Vorrichtung eine Angabe enthält, die dem LookUp Server (6) und/oder dem Relay Server (7) eine Freischaltung für einen Zugriff für eine Fernwartung erlaubt.

Es folgen 2 Blatt Zeichnungen

Anhängende Zeichnungen

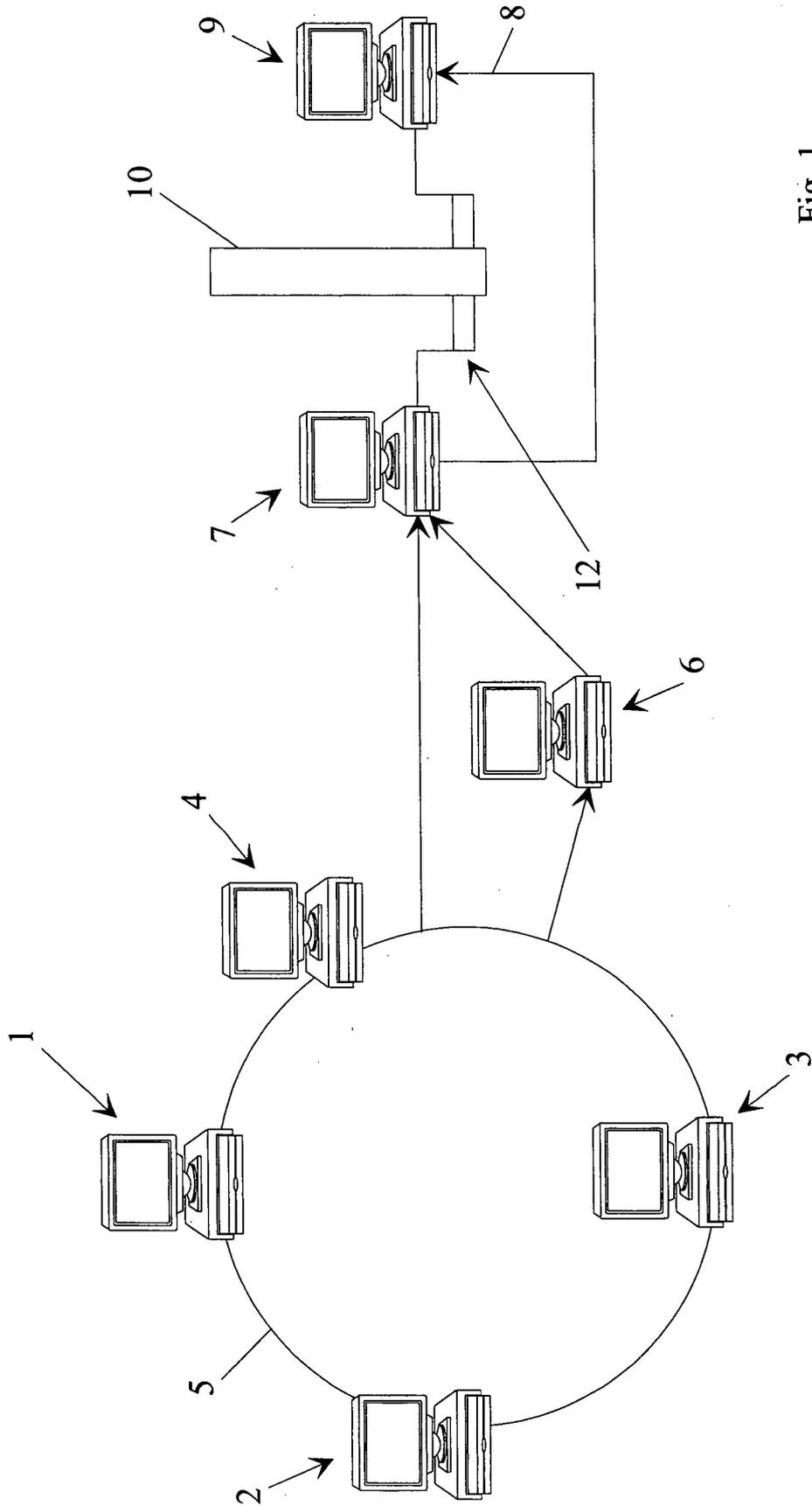


Fig. 1

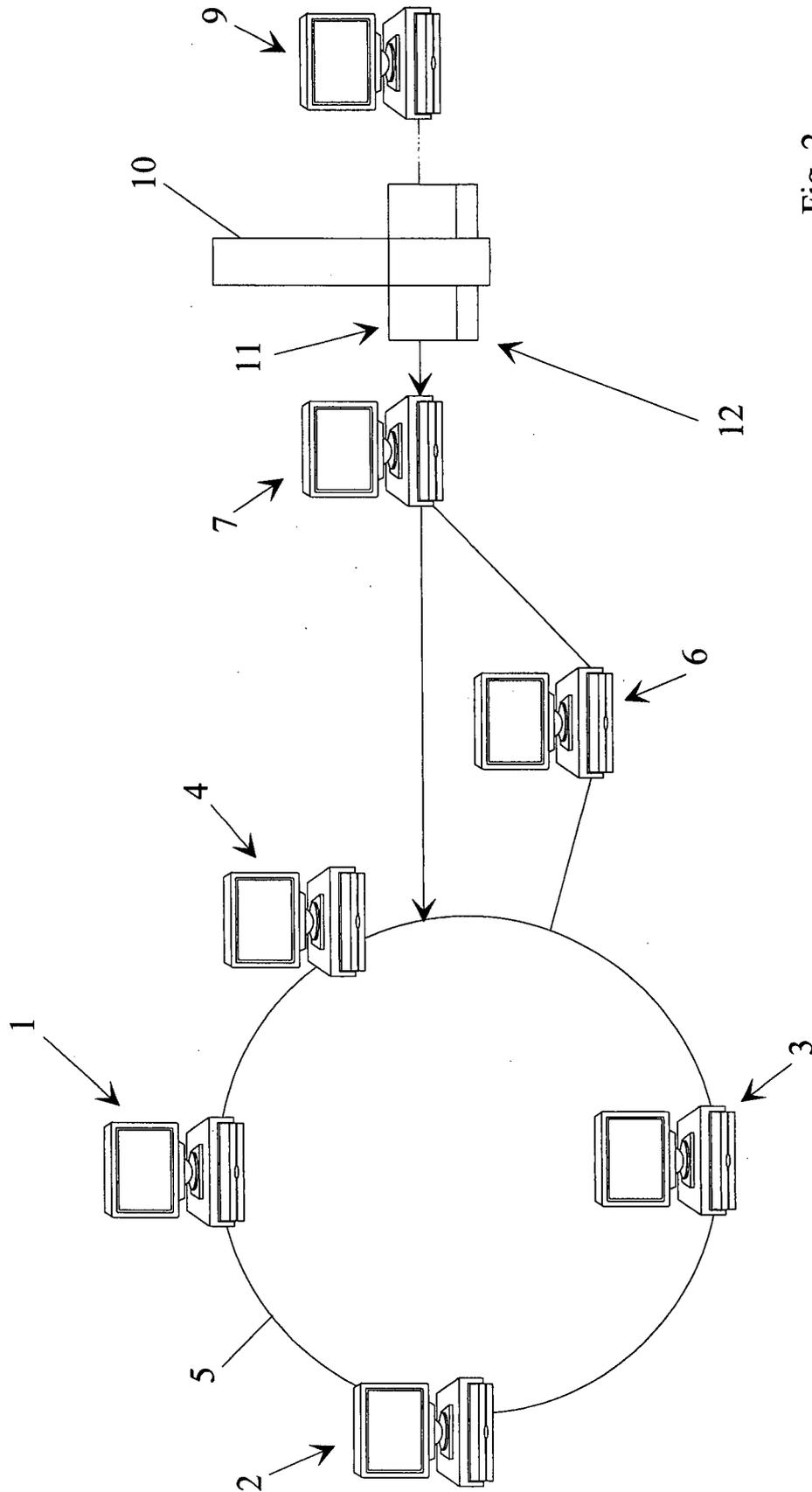


Fig. 2