REPÚBLICA FEDERATIVA DO BRASIL
MINISTÉRIO DA ECONOMIA
INSTITUTO NACIONAL DA PROPRIEDADE INDUSTRIAL

CARTA PATENTE Nº PI 0809809-3

O INSTITUTO NACIONAL DA PROPRIEDADE INDUSTRIAL concede a presente PATENTE DE INVENÇÃO, que outorga ao seu titular a propriedade da invenção caracterizada neste título, em todo o território nacional, garantindo os direitos dela decorrentes, previstos na legislação em vigor.

(21) Número do Depósito: PI 0809809-3

(22) Data do Depósito: 24/04/2008

(43) Data da Publicação do Pedido: 06/11/2008

(51) Classificação Internacional: G06F 9/06.

(30) Prioridade Unionista: US 11/740,617 de 26/04/2007.

(54) Título: "MÉTODO DE ACESSO A DADOS REMOTOS E SISTEMA DE ACESSO A DADOS REMOTOS"

(73) Titular: HEWLETT-PACKARD DEVELOPMENT COMPANY, L.P., Sociedade Americana. Endereço: 11445 COMPAQ CENTER DRIVE WEST, HOUSTON, TX 77070, ESTADOS UNIDOS DA AMÉRICA(US)

(72) Inventor: WAEL MOHAMAD IBRAHIM.

Prazo de Validade: 10 (dez) anos contados a partir de 19/03/2019, observadas as condições legais

Expedida em: 19/03/2019

Assinado digitalmente por:
Liane Elizabeth Caldeira Lage
Diretora de Patentes, Programas de Computador e Topografias de Circuitos Integrados

"MÉTODO DE ACESSO A DADOS REMOTOS E SISTEMA DE ACESSO A DADOS REMOTOS".

Histórico da Invenção

Dispositivos de computação móvel se tornaram onipresentes no mundo atual. Tais dispositivos, conquanto úteis e práticos, têm problemas referentes à segurança. Por exemplo, se um destes dispositivos for roubado, uma pessoa ou entidade não-autorizada acessar dados sensíveis armazenados remotamente do dispositivo, mas que são acessíveis à mesma. Em um cenário, esta pessoa ou entidade não-autorizada de posse ilegal de um notebook, pode usá-lo para acessar dados sensíveis armazenados em um servidor remoto.

Descrição Resumida dos Desenhos

Para uma descrição detalhada das configurações exemplares da presente invenção, faz-se referência aos desenhos anexos, nos quais:

A figura 1 mostra um sistema, de acordo com várias configurações; e

A figura 2 mostra um método, de acordo com várias configurações.

Notação e Nomenclatura

Certos termos usados na descrição e reivindicações anexas se referem a componentes de sistemas particulares. Aqueles habilitados na técnica deverão apreciar que as diversas companhias podem se referir ao mesmo componente com nomes diferentes. Este documento não distingue componentes de nome diferente, mas tendo a mesma função. Na descrição e nas reivindicações anexas, os termos "incluindo" e "compreendendo" são usados de modo amplo, que, portanto, devem ser interpretados como "incluindo, mas não se limitando". Também os termos "acoplar" e "acopla" se referem a meios de conexão elétrica sem-fio, a meios de conexão óptica, e a meios de conexão quer diretos ou indiretos. Assim, se um primeiro dispositivo conecta um segundo dispositivo, tal conexão pode ser feita por meio de conexão elétrica direta ou

indireta, ou por outros dispositivos e conexões, por uma conexão elétrica óptica, ou elétrica sem-fio. Aqui, o termo "sistema" se refere à combinação de dois ou mais componentes. Um sistema pode compreender, por exemplo, uma combinação de servidor e cliente, ou um servidor sozinho, ou mesmo um sub-sistema em um computador.

Descrição Detalhada da Invenção

A figura 1 mostra um computador servidor 10 comunicativamente acoplado a um computador cliente 30 através de uma rede 28. Em várias configurações, a rede 28 inclui Rede de Área Local (LAN de "Local Area Network"), Rede de Área Estendida (WAN de "Wide Area Network"), e outros tipos de rede. O servidor 10 compreende um processador 12 acoplado a um meio de armazenamento 14, e uma interface de rede 20. Pelo menos o processador 12 compreende uma lógica que, em várias configurações, executa parte ou toda a funcionalidade descrita nesta, que é atribuível ao computador servidor 10. O dispositivo de armazenamento 14 compreende um meio legível por computador, tal como uma memória volátil (i.e. memória de acesso randômico), meio de armazenamento não-volátil (disco rígido, memória Flash, ou memória de disco apenas de leitura (CD-ROM) etc.), ou uma combinação destes. O meio de armazenamento 14 compreende um ou mais itens de dado 16 acessíveis ao computador cliente 30, a luz dos vários mecanismos descritos, e, ademais, pode ser junto ou separado do computador servidor 10.

O computador cliente 30 compreende um processador 32, um ou mais recursos de hardware 34, um ou mais recursos de software 36, um meio legível por computador 38 (CRM de Computer Readable Media"), interface de rede 40, dispositivo de entrada 42, e um meio legível por computador 44. Em várias configurações, o computador cliente 30 também compreende um dispositivo de determinação de localização 50. Em várias configurações, o dispositivo de determinação de localização 50 compreende um receptor de Sistema de Posicionamento

Global (GPS de "Global Positioning System") ou outros mecanismos, que propiciem ao computador cliente 30 determinar sua localização física em uma sala, edifício, cidade, ou qualquer lugar no mundo (dentro da capacidade do dispositivo de determinação de localização).

O dispositivo de entrada compreende mouse, trackball, teclado, ou outros tipos de dispositivos de entrada. O dispositivo de saída 44 compreende uma tela ou outros tipos de dispositivo, através dos quais um usuário de computador cliente 30 tem acesso a um ou mais itens de dados 16 armazenados no computador servidor 10. Usando um dispositivo de entrada 41 e um dispositivo de saída 44, o usuário do computador cliente 30 pode acessar um ou mais itens de dados 16 no computador servidor 10.

O computador servidor 10 e o computador cliente 30 compreendem uma interface de rede (interfaces 20 e 40). As interfaces de rede 20 e 40 permitem que o computador servidor e computador cliente 10 e 30 se comuniquem através da rede 28. Em várias configurações, cada interface compreende um Controlador de Interface de Rede (NIC de "Network Interface Controller").

Os recursos de hardware 34 no computador servidor 30 compreendem vários recursos configuráveis, tais como, memória, portas de Entrada/Saída I/O (Input/Output), etc.. Os recursos de software 36 compreendem tais recursos como um ou mais sistemas operacionais possivelmente diferentes (Windows, LINUX, etc.), e vários aplicativos, assinaturas de vírus, versões de Sistema Básico de Entrada/Saída (BIOS de "Basic Input/Output System"), pacotes de serviço de sistema operacional, etc..

O meio legível por computador 38 compreende um código 45 executável pelo processador 32. Pelo menos o processador 32 que executa o código 45 inclui uma lógica que permite ao computador cliente 30 executar uma ou mais das ações descritas, que são atribuíveis ao computador cliente 30.

Em operação, o usuário de computador cliente 30 pede

acesso a um ou mais itens de dados 16 ao computador servidor 10. Em várias configurações, o computador servidor 10 faz o computador cliente 30 ativar uma "máquina virtual" específica antes de o servidor 10 prover os dados solicitados ao computador cliente 30. O computador cliente 30 é capaz de ativar uma ou mais múltiplas máquinas virtuais é um ambiente operacional que opera em conexão e de modo independente de um sistema operacional hospedeiro. Uma máquina virtual é um ambiente operacional auto-contido, que se comporta como um computador separado.

Ainda com referência à figura 1 e de acordo com várias configurações, um ou mais dos itens de dados 16 do computador servidor são associados a um particular Identificador de Máquina Virtual (VMI de "Virtual Machine Identifier") 18. O VMI 18 compreende um valor associado a uma certa máquina virtual que deve ser implementada (ativada) por um computador cliente 30, para o computador cliente 30 receber e acessar os dados correspondentes. Um VMI 18 compreende um número seqüencial, uma designação alfanumérica, ou qualquer outro tipo de valor para distinguir e identificar a máquina virtual de modo único. Em algumas configurações, todos os itens de dados 16 do computador servidor 10 são associados ao mesmo identificador virtual, enquanto em outras configurações, um ou mais itens de dados 16 são associados a um identificador de máquina virtual diferente daquele de um ou mais itens de dados 16. Alguns itens de dados 16 podem ser associados ao VMI 18, enquanto outros não são associados ao VMI 18.

Em algumas configurações, cada vez que um item de dado 16 é criado e armazenado no computador servidor 10, o usuário de computador servidor administrador designa ao item de dado recém-armazenado 16 um particular identificador de máquina virtual, que deve ser ativado pelo computador servidor 30 para o computador cliente 30 receber e prover o dado ao usuário. Desta maneira,

o requisito de segurança dos itens de dados subjacentes é mapeado para as máquinas virtuais desejadas, que devem ser usadas para acessar remotamente os itens de dados.

Quando da recepção do pedido de um particular item de dado 16 a partir do computador cliente 30, o processador 12 do computador servidor 10 obtém o identificador da máquina virtual associada ao item de dado pedido 16. O processador 12 então provê o identificador de máquina virtual 18 pela interface de rede 20 para o computador cliente 30 através da rede 28. O identificador de máquina virtual 18 é recebido pelo processador do computador cliente 32 através da interface de rede do computador cliente 40. O processador 32 do computador cliente 30 ativa a máquina virtual associada ao identificador de máquina virtual especificado pelo computador servidor 18. Uma vez ativada a máquina virtual especificada pelo processador, o servidor 10 provê o item de dado solicitado 16 para o computador cliente 30, que será apresentado ao usuário do computador cliente. Em várias configurações, a ativação da máquina virtual compreende ações, tais como, alocar uma quantidade de memória específica, carregar um particular sistema operacional, habilitar e desabilitar portas de entrada e saída, etc..

O código 45 compreende um monitor de máquina virtual (VMI de "Virtual Machine Monitor"), que ativa as máquinas virtuais apropriadas usando recursos de hardware e software 34 e 35. Em algumas configurações, mais que uma máquina virtual pode ser ativada por vez.

De acordo com várias configurações, o computador servidor 10 verifica se o computador cliente 30 ativou a máquina virtual correta antes de transmitir o item pedido 16 para o computador cliente 30. Um exemplo de verificação é o uso de um mecanismo baseado em um módulo de plataforma segura (TPM de "Trusted Plataform Module"), tal como aquele descrito na Publicação N° 2005/0235141 "Subordinate Trusted Plataform Module" incorporada nesta por referência. Por exemplo, o computador cliente 30

depois de ativar a máquina virtual específica, computa um ou mais valores ("metrics") da configuração resultante da máquina virtual recém-ativada do computador cliente, e provê um ou mais valores para o computador servidor 10 através da rede 28. O computador servidor 10 compara o valor recebido do computador cliente 30 com uma cópia legítima. Se não coincidir, o computador servidor 10, pelo menos em algumas configurações, não fornece o dado solicitado 16 ao computador cliente 30.

Outro mecanismo de segurança implementado no sistema mostrado na figura 1 faz o computador cliente 30 ativar a máquina virtual especificada pelo computador servidor, mas, apenas se o computador cliente 30 se localizar fisicamente no local correspondente à informação de localização associada à máquina virtual. Em pelo menos algumas configurações, o local se refere a uma localização geográfica, definida por coordenadas de longitude e latitude.

O meio legível por computador 38 compreende um conjunto de dados 46 que provê, para cada identificador de máquina virtual 47, a informação de localização 48. Cada informação de localização 48 especifica, em várias configurações, uma gama de localizações, onde deve estar o computador cliente 30 fisicamente, de modo que o computador cliente 30 possa ativar a máquina virtual associada ao identificador de máquina virtual 47. Em outras configurações, a informação de localização 48 define uma ou mais localizações, onde o computador servidor 30 não deve ativar a máquina virtual associada ao correspondente identificador de máquina virtual 47, portanto, especificando de modo indireto a localização admissível para a máquina virtual.

Com base na informação de localização 48, o processador 32 do computador cliente 30 compara a localização corrente do computador cliente provida, por exemplo, pelo dispositivo de determinação de localização 50, com a informação de localização 48 do CRM 38, para determinar

se o computador cliente 30 se encontra correntemente em um local que permita que o computador cliente ative a máquina virtual especificada pelo servidor. Se o computador cliente 30 estiver em um local adequado, como definido pelo conjunto de dados 46, o processador 32 ativa a máquina virtual especificada, mas se, ao invés, o computador cliente 30 não se encontrar em um local adequado que permita que o computador cliente ative a máquina virtual especificada, então o processador 32 impede a ativação da correspondente máquina virtual e, por conseguinte, o computador cliente 30 não recebe os itens de dados 16 solicitados do servidor 10.

A figura 2 ilustra um método, de acordo com várias configurações da invenção. As ações listadas na figura 2 podem ser seguidas em ordem diferente daquela mostrada, sendo que várias ações podem ser realizadas concomitantemente. Em 102, o método compreende receber um pedido para um certo item a partir do computador cliente 30. Em 104, o método adicionalmente compreende obter o identificador da máquina virtual associada ao dado pedido. Em 106, o método também compreende prover o identificador de máquina virtual a partir do computador servidor 10 para o computador cliente 30 pela rede 28.

Em 108, o computador cliente 30 determina se a sua localização é tal que a máquina virtual especificada pode ser ativada no computador cliente 30, mas se, ao invés, o computador cliente se encontrar em um local não adequado para ativar a máquina virtual especificada, então, em 110, o método impede que o computador cliente 30 ative a máquina virtual especificada. Adicionalmente, o computador cliente 30 pode alertar o computador servidor 10 sua incapacidade de ativar a máquina virtual especificada. Este alerta indica que o computador cliente 30 foi roubado. Em vista do recebimento deste alerta, a partir do computador cliente 30, o computador servidor não fornece o item solicitado pelo computador cliente 30. Adicionalmente ou alternativamente, o servidor 10 pode

desabilitar um ou mais mecanismos de segurança, tal como, por exemplo, o alerta para o administrador de rede que o computador cliente 30 solicitou um certo dado, mas falhou na ativação da máquina virtual correta.

Em 108, o computador cliente 30 pode determinar que sua localização corrente não se encontra na gama de localizações especificada, que permita que o computador cliente 30 ative a máquina virtual especificado pelo computador servidor 10. Daí, em 112, o método adicionalmente compreende a etapa de fazer o computador cliente 30 ativar a máquina virtual especificada. Em 114, o servidor 10 verifica se o computador cliente 30 ativou a máquina virtual correta, de acordo com o identificador de máquina virtual provido para o computador cliente 30 pelo computador servidor 10. Em 116, o servidor 10 permite ao computador cliente 30 acessar o item de dado, transmitindo este item de dado ao computador cliente 30, se o servidor 10 determinar que o computador ativou a máquina virtual correta.

Na configuração mostrada na figura 1, o computador cliente 30 inclui um dispositivo de determinação de localização 50, através do qual o computador cliente 30 determina sua localização corrente. Em outras configurações, o mecanismo para determinar a localização do computador cliente 30, não faz parte do mesmo, mas, ao invés, é separado deste. Por exemplo, deve ser implementado um serviço de atestado de localização (LAS) para determinar se a localização do computador cliente corresponde ao requisito de localização especificado para o dado pretendido pelo usuário do computador cliente. Um exemplo de tal serviço de atestado de localização LAS pode ser encontrado no Pedido de Patente co-pendente "Location Attestation Service", N° de Série 11/709473, incorporado nesta por referência. Através do LAS, o computador cliente 30 aplica um pedido de dado do computador servidor ao servidor 10. O servidor 10 solicita a prova de localização do computador cliente 30.

O computador cliente 30 busca um dispositivo de interface de serviço de atestado de localização (LASID) (um LASID por área de localização), que contata um servidor de administração, que pode ser um computador servidor 10 ou um outro servidor, e concede um certificado de localização para o dispositivo de computador cliente 30. O computador cliente 30 então fornece o certificado de localização para o servidor 30, e através do qual se verifica se a localização do computador cliente permite a ativação da máquina virtual.

De acordo com outro exemplo, a decisão 108 da figura 2 é realizada pelo computador servidor 10, solicitando a localização do computador cliente 30 para o computador cliente 30. O computador cliente 30 fornece sua localização ao computador servidor 10. O computador servidor 10 compara a localização fornecida com a informação de localização que pode estar especificada para cada item de dado 16. Assim, nesta configuração, cada item de dado 16 compreende um identificador de máquina virtual 18, que especifica a máquina virtual que deve ser ativada pelo computador cliente 30, assim como a informação de localização que define a localização na qual a correspondente máquina virtual pode ser ativada pelo computador servidor 30. Se o servidor 10 determinar que o computador cliente 30 se encontra no local correto, o servidor 10 retransmite um sinal de volta para o computador cliente 30, autorizando o computador cliente 30 a ativar a máquina virtual definida pelo servidor 10. Caso contrário, o servidor 10 impede que o computador cliente 30 ative a máquina virtual especificada.

De acordo com várias configurações, o computador cliente 30 monitora sua localização e termina a máquina virtual ativada, se o computador cliente 30 sair de onde se permite a ativação da máquina virtual. A terminação da máquina virtual destrói partições da máquina virtual, assim como as chaves e segredos associados. Portanto, se o computador cliente 30 (um computador móvel)

se deslocar, com a máquina virtual ativa, o computador cliente 30 termina a máquina virtual, se esta não for permitida na nova localização. O computador cliente 30, ou qualquer dispositivo separado que determine a localização do computador cliente e garanta que a localização seja apropriada para a máquina virtual especificada, quer em regime contínuo ou periódico (uma vez *per* minuto, a cada 5 minutos, etc.), ou através de um mecanismo condicionado a evento, tal como, por exemplo, pela perda do sinal de localização a partir de um dispositivo de determinação de localização, monitora a localização em conformidade com o requisito de localização do dado de servidor acessado pelo computador cliente 30.

A especificação tem um caráter meramente ilustrativo dos princípios e configurações da presente invenção. Numerosas variações e modificações da mesma serão aparentes àqueles habilitados na técnica, depois apreciar devidamente a especificação. Pretende-se que as reivindicações anexas englobem todas tais variações e modificações.

REIVINDICAÇÕES

1- Método de acesso a dados remotos compreendendo:

receber (102) um pedido de dado a partir de um computador cliente (30);

obter (104) um identificador de uma máquina virtual, o citado identificador de máquina virtual associado ao citado dado; e

prover (106) o citado identificador de máquina virtual para o computador cliente,

o método **caracterizado** pelo fato de o computador cliente ativar (112) uma máquina virtual de acordo com o citado identificador de máquina virtual; e

verificar (114) se o computador cliente ativou uma máquina virtual de acordo com o citado identificador de máquina virtual.

2- Método, de acordo com a reivindicação 1, **caracterizado** pelo fato de que compreende ainda computar um valor associado à citada máquina virtual.

3- Método, de acordo com a reivindicação 1, **caracterizado** pelo fato de que compreende ainda utilizar a informação de localização para determinar (108) se uma máquina virtual associada ao citado identificador de máquina virtual deve ser ativada.

4- Sistema de acesso a dados remoto (30) compreendendo:

uma lógica; e

uma interface de rede (40) acoplada à citada lógica; em que a citada lógica envia um pedido de dados através de uma rede via interface de rede e recebe uma resposta ao citado pedido, a citada resposta compreende um identificador de uma máquina virtual, citado identificador de máquina virtual associado ao dado solicitado;

o sistema **caracterizado** pelo fato de que a lógica é adaptada para ativar uma máquina virtual de acordo com o citado identificador de máquina virtual e para fornecer informação através da rede pela qual um dispositivo remoto pode verificar

que o sistema ativou a máquina virtual de acordo com o citado identificador de máquina.

5- Sistema, de acordo com a reivindicação 4, **caracterizado** pelo fato de que a citada lógica determina se ativa a máquina virtual de acordo com o citado identificador de máquina virtual com base em se o sistema está em uma localização na qual a citada máquina virtual é permitida ser ativada.

6- Sistema, de acordo com a reivindicação 4, **caracterizado** pelo fato que compreende ainda um dispositivo de determinação de localização (50) que fornece uma localização do sistema para a citada lógica, e a citada lógica determina se ativa a máquina virtual com base na citada localização do sistema.

7- Sistema, de acordo com a reivindicação 4, **caracterizado** pelo fato de que compreende ainda um meio de armazenamento (38), para pelo menos uma máquina virtual, uma localização na qual a citada pelo menos uma máquina virtual pode ser ativada.

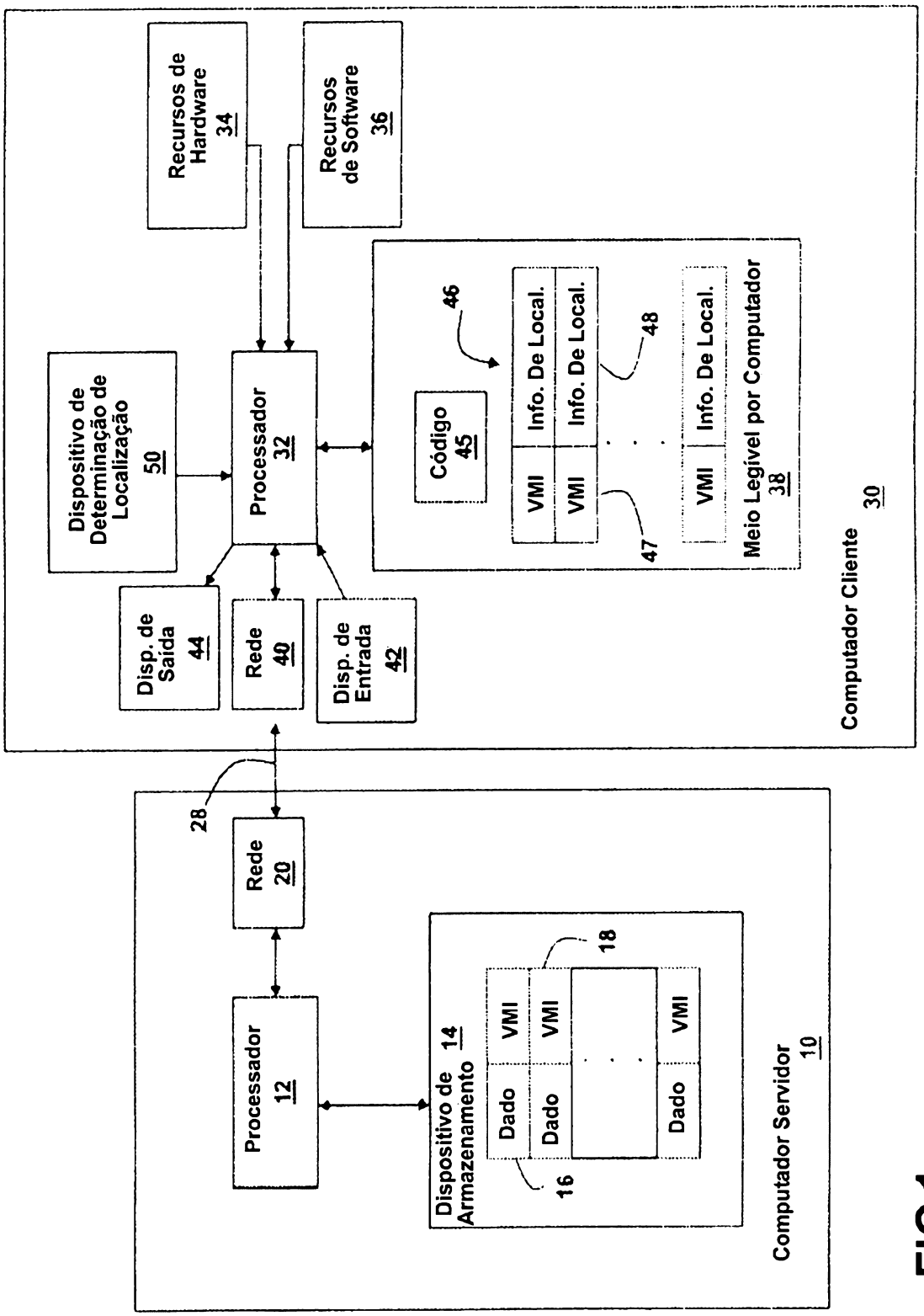
Computador Cliente 30
Recursos de Hardware 34
Recursos de Software 36
Dispositivo de Determinação de Localização 50
Processador 32
Código 45
46
Info. De Local.
VMI
48
47
Meio Legível por Computador 38
Disp. de Saída 44
Rede 40
Disp. de Entrada 42
28
Rede 20
Processador 12
Dispositivo de Armazenamento 14
Dado
VMI
18
16
Computador Servidor 10

FIG.1

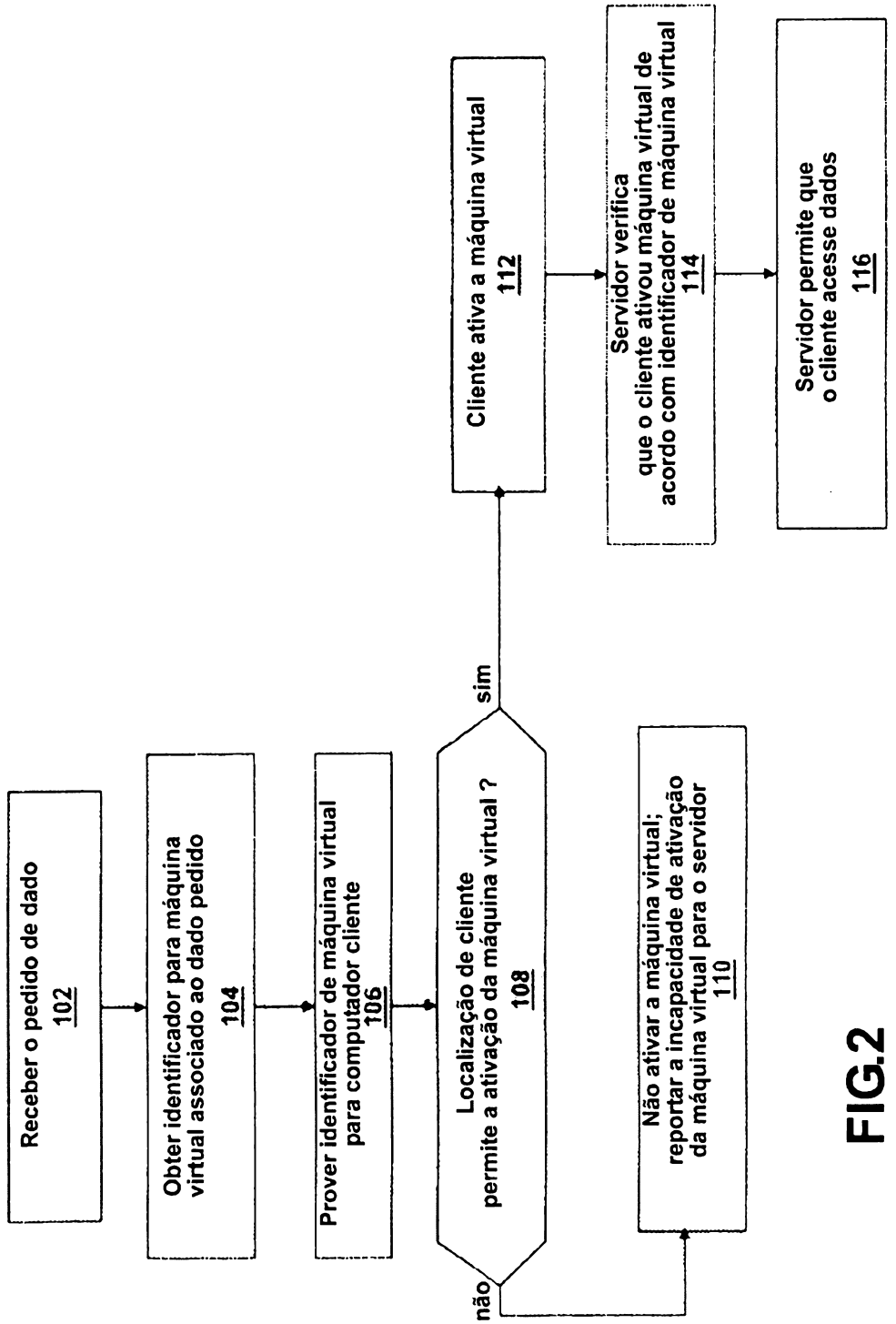
Receber o pedido de dado
102
Obter identificador para máquina virtual associado ao dado pedido
104
Prover identificador de máquina virtual para computador cliente
106
Localização de cliente permite a ativação da máquina virtual ?
108
sim
não
Cliente ativa a máquina virtual
112
Servidor verifica que o cliente ativou máquina virtual de acordo com identificador de máquina virtual
114
Servidor permite que o cliente acesse dados
116
Não ativar a máquina virtual; reportar a incapacidade de ativação da máquina virtual para o servidor
110

FIG.2