República Federativa do Brasil
Ministério do Desenvolvimento, Indústria
e do Comércio Exterior
Instituto Nacional da Propriedade Industrial.

(11) **PI9612331-1 B1**

BRPI9612331B1

(22) Data de Depósito: 04/12/1996
(45) Data da Concessão: 23/08/2011
(RPI 2120)

(51) Int.Cl.:
G06F 11/00 2006.01
G06F 11/08 2006.01
G06F 11/14 2006.01
G06F 11/34 2006.01
G06F 3/00 2006.01
G06F 13/00 2006.01
G06F 15/163 2006.01

(54) Título: **APARELHO E MÉTODO DE SEGURANÇA PARA UM SISTEMA DE PROCESSAMENTO DE DADOS.**

(30) Prioridade Unionista: 28/12/1995 US 08/580.136

(73) Titular(es): Sterling Commerce, Inc.

(72) Inventor(es): Christopher Von See, S. Dale Ander

"APARELHO E MÉTODO DE SEGURANÇA PARA UM SISTEMA DE PROCESSAMENTO DE DADOS"

CAMPO TÉCNICO DA INVENÇÃO

Essa invenção refere-se em geral ao campo dos sistemas de processamento de dados, e mais especificamente a um aparelho e método de segurança para um sistema de processamento de dados.

HISTÓRICO DA INVENÇÃO

Muitos sistemas de processamento de dados incluem uma coleção de dispositivos interconectados. As capacidades de armazenagem e processamento desses sistemas podem ser distribuídas entre esses dispositivos interconectados. Um usuário em um primeiro dispositivo em um sistema desse tipo pode desejar acessar as capacidades de armazenagem ou processamento de um segundo dispositivo no sistema.

A medida que os sistemas de processamento tornam-se maiores e mais complexos para servir a uma variedade de usuários, os administradores de sistema podem desejar restringir o acesso às capacidades de armazenagem e processamento dos dispositivos do sistema. Uma técnica de segurança conhecida permite aos usuários acesso irrestrito a dispositivos de sistema com o fornecimento de informação de acesso apropriada, tal como um identificador e uma senha. Entretanto, os usuários desautorizados podem frustar essa técnica de

segurança apropriando-se da informação de acesso. Além disso, essa técnica de segurança pode não proporcionar designações de acesso específicas do usuário.

SUMÁRIO DA INVENÇÃO

De acordo com a presente invenção, as desvantagens e problemas associados com segurança em um sistema de processamento de dados foram substancialmente reduzidos ou eliminados.

De acordo com uma configuração da presente invenção, um sistema de processamento inclui um nodo de submissão tendo um identificador. Um nodo de processamento está acoplado ao nodo de submissão e inclui uma memória que armazena um representante associado com o nodo de submissão. O representante especifica uma localização na memória do nodo de processamento acessível pelo nodo de submissão. O nodo de processamento recebe o identificador do nodo de submissão e fornece o acesso do nodo de submissão ao nodo de processamento de acordo com o representante.

Vantagens técnicas importantes da presente invenção incluem manter em um nodo de processamento um representante para um nodo de submissão querendo acessar as capacidades de armazenagem ou processamento do nodo de processamento. O representante inclui um ou mais parâmetros de acesso que podem especificar uma localização na memória do nodo de processamento que é

acessível pelo nodo de submissão. Os parâmetros de acesso podem ser armazenados como um representante associado com um nodo de submissão ou um usuário de um nodo de submissão. Uma outra vantagem técnica importante inclui fornecer ambos, um representante à distância e um representante local para especificar os parâmetros de acesso do nodo de submissão. Em uma configuração, os primeiros parâmetros de acesso especificados em um representante à distância levam procedência sobre segundos parâmetros de acesso especificados em um representante local. Nessa maneira, o representante local estabelece parâmetros de acesso da linha de base para uma classe de usuários e o representante à distância designa os parâmetros de acesso específicos do usuário.

BREVE DESCRIÇÃO DOS DESENHOS

Para um entendimento mais completo da presente invenção e para aspectos e vantagens adicionais, é feita agora referência à descrição seguinte tomada em conjunto com os desenhos que a acompanham, nos quais:

a FIGURA 1 ilustra um sistema de processamento de dados construído de acordo com os ensinamentos da presente invenção;

a FIGURA 2 ilustra um representante à distância e um representante local usados em um sistema

de processamento de dados construído de acordo com os ensinamentos da presente invenção; e

a FIGURA 3 ilustra um fluxograma de um método para operar um sistema de processamento de dados construído de acordo com os ensinamentos da presente invenção.

DESCRIÇÃO DETALHADA DA INVENÇÃO

A FIGURA 1 ilustra um sistema de processamento de dados 10 que inclui um nodo de processamento 12 acoplado aos nodos de submissão 14 e 16, e um nodo de processamento 18 acoplado aos nodos de submissão 20 e 22. Em uma configuração, os nodos de processamento 12 e 18 podem ser dois sistemas separados de processamento de dados acoplados por um elo. Ambos, os nodos de processamento 12 e 18 e os nodos de submissão 14, 16, 20, e 22 são referidos geralmente como dispositivos. Os nodos de submissão 14, 16, 20 e 22 querem acessar os nodos de processamento 12 e 18. Em geral, o sistema 10 gerencia a colocação e acesso às capacidades de armazenagem e processamento dos nodos de processamento 12 e 18.

Os nodos de submissão 14, 16, 20 e 22 podem ser computadores ou outros dispositivos com capacidades de armazenagem e processamento, mas podem também ser terminais ou outros dispositivos de entrada/saída sem armazenagem local significante ou capacidades de

processamento. Os nodos de submissão 14, 16, 20, e 22, embora mostrados de forma ilustrativa como dispositivos separados, também podem ser programas ou instruções operando em nodos de processamento 12 e 18. Em geral, os nodos de submissão 14, 16, 20 e 22 podem ser qualquer entidade lógica em hardware e/ou software, separada ou integral ao seu nodo de processamento associado 12 ou 18, que fornece acesso às capacidades de armazenagem e processamento dos nodos de processamento 12 e 18.

O nodo de processamento 12 é acoplado aos nodos de submissão 14 e 16 usando um primeiro circuito de interface 24. Um segundo circuito de interface 26 acopla o nodo de processamento 12 ao nodo de processamento 18 usando o elo 28. Um processador 30 e uma memória 32 são acoplados ao primeiro circuito de interface 24 e segundo circuito de interface 26 usando o barramento 34.

A memória 32 pode ser qualquer memória adequada, tais como memória de acesso randômico dinâmica ou estática (RAM), memória somente de leitura (ROM), meios magnéticos, meios óticos, CD-ROM, ou outros meios de armazenagem adequados voláteis ou não voláteis. A memória 32 armazena informação em arquivos, diretórios, ou qualquer outro arranjo adequado que pode ser acessado pelo primeiro circuito de interface 24,

segundo circuito de interface 26, ou processador 30. A memória 32 contém instruções para a execução pelo processador 30 para gerenciar a operação do nodo de processamento 12.

A memória 32 também contém listas de representantes que especificam o acesso do usuário às capacidades de armazenagem e processamento do nodo de processamento 12.. Um representante compreende um ou mais parâmetros de acesso associados com um dispositivo ou usuário de um dispositivo no sistema 10. Os parâmetros de acesso podem incluir autorizações de leitura e escrita, autorizações de processamento, especificações de arquivo ou diretório, limitações de localização de arquivo, limitações de localização de processamento, ou qualquer outra informação que especifica acesso ou disponibilidade das capacidades de armazenagem e processamento do nodo de processamento 12.

Os parâmetros de acesso residindo na memória 32 do nodo de processamento 12 podem ser organizados em uma lista de representantes à distância 36 e uma lista de representantes locais 38, que são descritos em mais detalhe com referência à Figura 2. Os representantes à distância 36 são associados com os dispositivos no sistema 10 que são revisados remotamente pelo nodo de processamento 12, tal como o

nodo de processamento 18 e nodos de submissão 20 e 22. Representantes locais 38 são associados com dispositivos que são revisados localmente pelo nodo de processamento 12, tal como nodos de submissão 14 e 16. Os representantes locais 38 podem também ser associados com usuários diretos do nodo de processamento 12 que não operam um nodo de submissão. Os representantes à distância 36 e os representantes locais 38 podem também ser associados com programas e instruções operando nos nodos de processamento 12 e 18. Os representantes à distância 36 e os representantes locais 38 podem, além de ou ao invés de sua associação com um dispositivo, serem associados com o usuário do dispositivo.

O nodo de processamento 18 é acoplado aos nodos de submissão 20 e 22 usando um primeiro circuito de interface 40. Um segundo circuito de interface 42 acopla o nodo de processamento 18 ao nodo de processamento 12 usando o elo 28. Um processador 44 e uma memória 46 são acoplados ao primeiro circuito de interface 40 e segundo circuito de interface 42 usando um barramento 48.

A memória 46 pode ser qualquer meio de armazenagem adequado como discutido acima com referência à memória 32 no nodo de processamento 12. A memória 46 armazena informação em arquivos, diretórios, ou qualquer outro arranjo adequado que pode ser

acessado pelo primeiro circuito de interface 40, segundo circuito de interface 42, ou processador 44. A memória 46 contém instruções para execução pelo processador 44 para gerenciar a operação do nodo de processamento 18.

A memória 46 também contém uma lista de representantes que especificam o acesso do usuário às capacidades de armazenagem e processamento do nodo de processamento 18. Cada representante compreende um ou mais parâmetros de acesso associado com um dispositivo ou usuário de um dispositivo no sistema 10. Os parâmetros de acesso podem ser organizados em uma lista de representantes à distância 50 e uma lista de representantes locais 52. Os representantes à distância 50 são associados com dispositivos que são revisados remotamente pelo nodo de processamento 18, tal como nodo de processamento 12 e nodos de submissão 14 e 16. Os representantes locais 52 são associados com dispositivos revisados localmente pelo nodo de processamento 18, tais como nodos de submissão 20 e 22. Os representantes locais 52 podem também ser associados com usuários diretos do nodo de processamento 18 que não operam um nodo de submissão. Os representantes à distância 50 e os representantes locais 52 podem também ser associados com programas e instruções operando em nodos de processamento 12 e 18. Os representantes à

distância 50 e os representantes locais 52 podem, além de ou ao invés de sua associação com um dispositivo, serem associados com o usuário do dispositivo.

Em operação, o sistema 10 gerencia a localização das e acesso às capacidades de armazenagem e processamento dos nodos de processamento 12 e 18. Em uma configuração, os nodos de submissão 14, 16, 20 e 22 podem querer identificar um usuário ou interagir com os nodos de processamento 12 e 18. Os nodos de submissão 14, 16, 20 e 22 podem gerar instruções para serem executadas pelos nodos de processamento 12 e 18. Essas instruções podem ser organizadas como um processo a ser executado nos nodos de processamento 12 e 18 ou podem ser geradas pelo usuário de um nodo de submissão enquanto interagindo com um nodo de processamento. As instruções geradas pelos nodos de submissão 14, 16, 20 e 22 podem incluir comandos para executar um trabalho ou tarefa, copiar arquivos, submeter processos adicionais, ou executar qualquer outra tarefa adequada nos nodos de processamento 12 e 18.

As instruções ou processos submetidos incluem um identificador do nodo de submissão ou o usuário do nodo de submissão que é especificado ou indiretamente na transmissão ou diretamente por uma declaração de identificação específica. Os nodos de processamento 12 e 18 usam o identificador para recuperar representantes

à distância e representantes locais associados com o nodo de submissão ou o usuário do nodo de submissão e utilizam esses representantes para restringir o acesso a suas capacidades de armazenagem e processamento.

Por exemplo, o nodo de submissão 14 pode ser qualquer entidade lógica em hardware e/ou software, quer integral a ou separada do nodo de processamento 12, que quer acessar as capacidades de armazenagem e processamento do nodo de processamento 12. Na configuração onde o nodo de submissão 14 é separado do nodo de processamento 12, o identificador do nodo de submissão 14 está comunicado com o primeiro circuito de interface 24 do nodo de processamento 12. Em resposta ao recebimento do identificador, o nodo de processamento 12 recupera um representante local 38 armazenado na memória 32 que está associada com o nodo de submissão 14 ou o usuário do nodo de submissão 14. O representante inclui parâmetros de acesso especificando, por exemplo, uma localização na memória 32 do nodo de processamento 12 que pode ser acessado pelo nodo de submissão 14. O nodo de processamento 12 então proporciona ao nodo de submissão 14 acesso a suas capacidades de armazenagem e processamento de acordo com os parâmetros de acesso especificados no representante local 38.

Em um outro exemplo, o nodo de submissão 16 tendo um identificador quer acessar o nodo de processamento 18. O identificador está em comunicação com o primeiro circuito de interface 24 do nodo de processamento 12, que depois comunica o identificador ao segundo circuito de interface 26 usando o barramento 34. Se o nodo de processamento 12 já não está referenciado no identificador recebido do nodo de submissão 16, o nodo de processamento 12 pode modificar ou suprir o identificador do nodo de submissão 16 para incluir uma identificação do nodo de processamento 12. Em uma configuração específica, o identificador do nodo de submissão 16 compreende um primeiro identificador associado com o nodo de submissão 16 e um segundo identificador associado com o nodo de processamento 12. Por exemplo, se o nome do nodo de submissão 16 é "MIKE" e o nome do nodo de processamento 12 é "À DISTÂNCIA", então o identificador poderia ser "MIKE@À DISTÂNCIA".

O identificador gerado pelo nodo de submissão 16 e opcionalmente modificado ou suprido pelo nodo de processamento 12 é depois comunicado através do elo 28 ao segundo circuito de interface 42 do nodo de processamento 18. Com o recebimento do identificador, o nodo de processamento 18 acessa um representante à distância 50 armazenado na memória 46 que está associado com o nodo de submissão 16 ou o usuário do

nodo de submissão 16. Em uma configuração, o nodo de processamento 18 proporciona ao nodo de submissão 16 acesso a suas capacidades de armazenagem e processamento de acordo com os parâmetros de acesso especificados no representante à distância 50.

O nodo de submissão 16 pode fornecer informação ao nodo de processamento 18 para cancelar o mecanismo para determinação de um representante. Nesse caso, o representante à distância 50 no nodo de processamento 18 é desviado e ou o representante local 52 no nodo de processamento 18 é usado, ou nenhum representante de qualquer modo. O representante local específico 52 a ser usado é determinado pela informação cancelada fornecida pelo nodo de submissão 16. Em uma configuração específica, a informação cancelada é especificada usando uma declaração "SNODEID" ou "REMOTEID".

Em uma outra configuração, o representante à distância 50 associado com o nodo de submissão 16 ou o usuário do nodo de submissão 16 inclui um identificador local. O identificador local é associado com um representante local 52 que estabelece um ou mais parâmetros de acesso de linha de base. O representante à distância 50 pode então fornecer um ou mais parâmetros de acesso que adicionalmente especificam ou modificam os parâmetros de acesso no representante

local 52. Nessa maneira, o nodo de processamento 18 mantém um gabarito ou parâmetros de acesso de linha de base especificados no representante local 52 que aplicam-se a uma classe de usuários tais como hóspedes à distância, ou uma classe de dispositivos tais como dispositivos revisados localmente pelo nodo de processamento 12. Esse gabarito pode ser adicionalmente preparado para o usuário pelos parâmetros de acesso no representante à distância 50 associados com um nodo de submissão específico 16 ou um usuário específico do nodo de submissão 16.

Ambos os representantes à distância 50 e os representantes locais 52 podem ser ou específicos ou gerais na sua associação com um nodo de submissão. Um representante à distância específico 50 pode ser associado, por exemplo, com o nodo de submissão 16 que tem um identificador "MIKE@À DISTÂNCIA". Ao contrário, um representante à distância geral 50 pode aplicar-se a qualquer nodo de submissão que deseja acesso ao nodo de processamento 18. Na configuração específica onde o nodo de submissão 16 é identificado usando um primeiro e segundo identificador, o nodo de processamento 18 pode manter um representante específico, ou à distância ou local, que combina ambos o primeiro identificador e o segundo identificador, um representante mais geral que combina o primeiro identificador ou o segundo

identificador, ou o representante mais geral que aplica-se a todos os nodos de submissão 16. Nessa maneira, representantes específicos e gerais proporcionam flexibilidade a grupos associados de usuários com parâmetros de acesso definidos.

Os nodos de processamento 12 e 18 podem também desejar acessar as capacidades de armazenagem ou processamento de um outro dispositivo no sistema 10. Por exemplo, o nodo de processamento 12 tendo um identificador pode desejar acessar o nodo de processamento 18. Com o recebimento do identificador, o nodo de processamento 18 acessa um representante à distância 50 associado com o nodo de processamento 12 ou um usuário do nodo de processamento 12, e opcionalmente um representante local 52, e determina os parâmetros de acesso pertinentes. A presente invenção contempla ambos os acessos local ou remoto de um dispositivo por um outro dispositivo no sistema 10.

A FIGURA 2 ilustra o conteúdo do representante à distância 50 e do representante local 52 armazenado na memória 46 no nodo de processamento 18. Para propósitos de discussão, o representante à distância 50 e representante local 52 são associados com um usuário do nodo de submissão 16 que deseja acessar o nodo de processamento 18. Por exemplo, o usuário do nodo de submissão 16 pode desejar

identificar um usuário ou interagir com o nodo de processamento 18. O usuário do nodo de submissão 16 pode submeter, tanto interativamente quanto em lote, instruções ou processos para execução no nodo de processamento 18. O representante à distância 50 inclui um identificador 100 que identifica o usuário do nodo de submissão 16. Por exemplo, o identificador "MIKE@À DISTÂNCIA" especifica que o usuário do nodo de submissão 16 é chamado "MIKE" e do nodo de processamento 12 é chamado "À DISTÂNCIA". O representante à distância 50 também inclui um identificador local 102 que associa o usuário do nodo de submissão 16 com o representante local 52.

Com o recebimento do identificador do usuário do nodo de submissão 16, o nodo de processamento 18 refere o usuário do nodo de submissão 16 a um identificador local 102. A translação de um usuário à distância "MIKE@À DISTÂNCIA" para um usuário local válido "HÓSPEDE" proporciona um nível de segurança adicional desde que nem o nodo de submissão 16 nem o nodo de processamento 12 tem acesso ao identificador local 102 mantido no nodo de processamento 18. Qualquer mecanismo de segurança adicional permitido para o "HÓSPEDE" pelo nodo de processamento 18, tal como a segurança do sistema de

operação, pode ser aceito para suplementar a segurança fornecida pelo representante.

Os parâmetros de acesso no representante local 52 aplicam-se ao usuário do nodo de submissão 16 devido à translação do "MIKE@À DISTÂNCIA" para "HÓSPEDE". O representante local 52 inclui um identificador 104 que corresponde com o identificador local 102 do representante à distância 50. Ambos, o representante à distância 50 e o representante local 52 incluem autorizações funcionais que definem qual o nodo de submissão de autoridade funcional 16 é admitido para as capacidades de armazenagem e processamento do nodo de processamento 18, bem como, como essa autoridade funcional pode ser exercitada. Por exemplo, uma autoridade funcional especificada no representante à distância 50 ou representante local 52 pode incluir uma indicação de se o nodo de submissão 16 pode enviar um arquivo, receber um arquivo, submeter, executar, ou desempenhar alguma outra função ou comando no nodo de processamento 16. Informação adicional, tal como especificações de diretório, limitações de comando, limitações de leitura/escrita, limitações de armazenagem ou processamento, e outros, pode ser fornecida para adicionalmente definir como as funções autorizadas podem ser exercitadas.

Uma autorização de envio de arquivo (upload) 106 indica se o usuário do nodo de submissão 16 pode armazenar informação na memória 46 do nodo de processamento 18, e um diretório de envio de arquivo 108 especifica um diretório ou outra localização de memória adequada no nodo de processamento 18 que pode armazenar informação recebida do usuário do nodo de submissão 16. Similarmente, uma autorização de recebimento de arquivo (download) 110 indica se o usuário do nodo de submissão 16 pode receber informação armazenada na memória 46 do nodo de processamento 18, e um diretório de recebimento de arquivo 112 especifica um diretório ou outra localização de memória adequada no nodo de processamento 18 que pode ser acessada pelo usuário do nodo de submissão 16 para receber informação. Se a autorização de envio de arquivo 106 indica autorização e o diretório de envio do arquivo 108 não é especificado, então o usuário do nodo de submissão 16 pode armazenar informação em qualquer porção da memória 46 do nodo de processamento 18 sem restrição. Similarmente, se a autorização de recebimento de arquivo 110 indica autorização e o diretório de recebimento do arquivo 112 não é especificado, então o usuário do nodo de submissão 16 pode receber informação armazenada em qualquer porção

da memória 46 do nodo de processamento 18 sem restrição.

O representante local 52 também inclui um diretório de funcionamento 114 que especifica um diretório ou outra localização adequada de memória na qual o usuário do nodo de submissão 16 pode executar programas, shells scripts (textos de software que age como interface de comunicação entre o usuário e o sistema operacional), ou outros executáveis no nodo de processamento 18. Segurança adicional pode ser mantida proibindo-se o usuário do nodo de submissão 16 de emitir comandos iniciando com um especificador de diretório, tal como uma barra diagonal (/) em um ambiente de operação UNIX, e restringir comandos para ficarem no diretório de funcionamento 114. Além disso, um administrador de sistema pode estabelecer segurança elevada gerenciando de perto os arquivos e conteúdo de arquivos mantidos no diretório de funcionamento 114.

Um diretório de submissão 116 especifica o diretório ou outra localização adequada de memória no nodo de processamento 18 na qual o usuário do nodo de submissão 16 pode submeter instruções ou processos ao nodo de processamento 18. Por exemplo, um conjunto de instruções comunicadas do nodo de submissão 16 e executadas no nodo de processamento 18 pode criar um processo adicional tendo instruções para serem

executadas em um outro nodo de processamento. O efeito corrente-margarida de submeter instruções dentro de instruções pode ser encorajado, limitado, ou evitado dependendo do diretório de submissão 116 especificado no representante local 52.

Em uma configuração, o representante local 52 designado como "HÓSPEDE" aplica-se geralmente a usuários de dispositivos à distância que desejam acesso ao nodo de processamento 18. Se os parâmetros de acesso específicos do usuário são desejados, o representante à distância 50 inclui parâmetros de acesso que levam precedência sobre os parâmetros de acesso especificados no representante local 52. Para o exemplo ilustrado na FIGURA 2, a autorização de envio de arquivo 118 de representante à distância 50 leva precedência sobre a autorização de envio de arquivo 106 do representante local 52, e o envio do arquivo pelo usuário do nodo de submissão 16 não é autorizado. Similarmente, o diretório de recebimento de arquivo 120 e diretório de funcionamento 122 no representante à distância 50 especificam diretórios diferentes que são acessíveis pelo usuário do nodo de submissão 16. Os parâmetros de acesso que não são especificados no representante à distância 50 são estabelecidos pelas entradas no representante local 52.

Alguns dos parâmetros de acesso no representante à distância 50 e representante local 52 especificam uma localização na memória do nodo de processamento, tal como uma especificação de diretório, que é acessível para o nodo de submissão 16. Por exemplo, se o nodo de submissão 16 deseja copiar um arquivo do nodo de processamento 18, então as especificações de autorização de recebimento de arquivo e diretório de recebimento de arquivo no representante à distância 50 e representante local 52 serão examinadas antes da cópia ser executada. Se a instrução de cópia especifica um diretório que não é acessível pelo nodo de submissão 16, então a instrução não será executada. Similarmente, o nodo de submissão 16 pode desejar executar um programa no nodo de processamento 18. Se a instrução de funcionamento especifica um diretório que é diferente da especificação do diretório de funcionamento no representante à distância 50 ou representante local 52, então a instrução não será executada. Embora parâmetros de acesso particular tenham sido especificados para o representante à distância 50 e o representante local 52, deve ser entendido que a presente invenção contempla qualquer parâmetro adequado de acesso que possa ser especificado para gerenciar a localização de, ou acesso

às capacidades de armazenagem ou processamento do nodo de processamento 18.

A estrutura hierárquica do representante à distância 50 e representante local 52 proporcionam várias vantagens técnicas. Por exemplo, um representante local geral 52 para um grupo de usuários pode ser estabelecido para especificar uma linha de base dos parâmetros de acesso. Uma lista de parâmetros de acesso mais ou menos restritiva pode então ser mantida em uma base usuário por usuário usando o representante à distância 50. O identificador 100 do representante à distância 50 pode ser especificado pelo nodo de submissão 16 ou o usuário do nodo de submissão 16, dessa forma permitindo acesso ao nodo de processamento 18 usando identificadores diferentes associados com representantes diferentes e parâmetros de acesso diferentes.

Por exemplo, o usuário do nodo de submissão 16 pode tentar acessar o nodo de processamento 18 usando o identificador "JOE@À DISTÂNCIA" ao invés de "MIKE@À DISTÂNCIA". Já que o nodo de submissão 16 pode usar o nodo de processamento 12 para acessar outros dispositivos no sistema 10, a última parte do identificador pode ser "À DISTÂNCIA" (o nome do nodo de processamento 12). O identificador 100 no representante à distância 50 pode ser especificado indiretamente em

comunicações entre o nodo de submissão 16 e o nodo de processamento 18 ou diretamente por uma declaração de identificação gerada no nodo de submissão 16. Além disso, o usuário do nodo de submissão 16 pode especificar um identificador que é local para o nodo de processamento 18.

Além disso, o nodo submetido 16 pode ser sujeito a representantes mantidos em ambos os nodos de processamento 12 e 18. Por exemplo, o nodo de submissão 16 pode desejar acessar as capacidades de armazenagem e processamento do nodo de processamento 18. O nodo de submissão 16 primeiro acessa o nodo de processamento 12 de acordo com os parâmetros de acesso especificados em um representante local 38 associado com o nodo de submissão 16. Se autorizado pelos parâmetros de acesso especificados no representante local 38, o nodo de submissão 16 então tenta acessar o nodo de processamento 18, de acordo com um ou uma combinação de representante à distância 50 e representante local 52. Portanto, o nodo de submissão 16 pode ser sujeito a dois níveis de parâmetros de acesso estabelecidos pelo representante no nodo de processamento 12 e no nodo de processamento 18. Nessa maneira, um nodo de submissão que deseja acessar um nodo de processamento através de uma série de nodos de processamento intervenientes pode ser submetido a segurança do representante em cada um

dos nodos de processamento na cadeia do sistema de comunicações.

A FIGURA 3 ilustra um fluxograma de um método para operar o sistema 10 de acordo com os ensinamentos da presente invenção. Por toda essa descrição, todas as referências ao nodo de submissão 16 aplicam-se igualmente a um usuário do nodo de submissão 16. O método começa na etapa 200, onde o nodo de submissão 16 tenta acessar o nodo de processamento 18. Como descrito acima, isso pode ser realizado primeiro obtendo-se com sucesso acesso ao nodo de processamento 12 de acordo com os parâmetros de acesso especificados pelo representante local 38.

Se o nodo de processamento 18 força a recuperação de um representante para o nodo de submissão 16 na etapa 202, então o nodo de processamento 18 determina se o nodo de submissão 16 forneceu uma declaração de identificação na etapa 204. Uma declaração de identificação especifica um identificador e opcionalmente uma senha para o nodo de submissão 16. Se uma declaração de identificação é encontrada na instrução na etapa 204, então o nodo de processamento 18 procura por um representante à distância 50 associado com a informação especificada na declaração de identificação na etapa 206.

Se um representante à distância correspondente 50 é encontrado, então o nodo de processamento 18 especifica os parâmetros de acesso para o nodo de submissão 16 com base no identificador local 102 no representante à distância 50 na etapa 208. Esses parâmetros de acesso podem ser recuperados de um representante local 52 associado com o identificador local 102. Os parâmetros de acesso no representante local 52 são então suplementados ou modificados pelos parâmetros de acesso especificados no representante à distância 50 na etapa 210. A informação de identificação dos parâmetros de acesso estabelecidos, tal como um identificador de usuário e opcionalmente uma senha, é validada na etapa 211 usando, por exemplo, os procedimentos de segurança do sistema de operação. Se a informação de identificação é validada na etapa 211, então é fornecido acesso do nodo de submissão 16 ao nodo de processamento 18 de acordo com os parâmetros de acesso estabelecidos e outras restrições de segurança no nodo de processamento 18, tal como segurança do sistema de operação, na etapa 212. Se a informação de identificação não é validada, então é recusado acesso do nodo de submissão 16 ao nodo de processamento 18 na etapa 216.

Se o nodo de submissão 16 não fornece uma declaração de identificação na etapa 204, então o nodo

de processamento 18 procura por um representante à distância 50 associado com o identificador do nodo de submissão 16 na etapa 214. Esse identificador pode ser especificado indiretamente ou inerentemente em comunicações entre o nodo de submissão 16 e o nodo de processamento 18. Se o representante à distância 50 é encontrado para o identificador, então o nodo de processamento 18 estabelece os parâmetros de acesso para o nodo de submissão 16 nas etapas 208 e 210, e é fornecido acesso do nodo de submissão 16 na etapa 212. Se o representante à distância 50 não é encontrado nas etapas 206 ou 214, então é negado acesso do nodo de submissão 16 ao nodo de processamento 18 na etapa 216.

Se o nodo de processamento 18 não força a recuperação de um representante para o nodo de submissão 16 na etapa 202, então o nodo de processamento 18 determina se o nodo de submissão 16 forneceu uma declaração de identificação na etapa 218. Se nenhuma declaração de identificação é encontrada, então o nodo de processamento 18 procura por um representante à distância 50 associado com o identificador do nodo de submissão 16 na etapa 214, especifica os parâmetros de acesso nas etapas 208 e 210, e fornece acesso na etapa 212.

Se uma declaração de identificação é encontrada na etapa 218, então o identificador e a

senha na declaração de identificação são validados na etapa 220. Se o identificador e senha na declaração de identificação são válidos na etapa 220, então os parâmetros de acesso são especificados com base no identificador na etapa 222. Alternativamente, com o fornecimento de um identificador e senha válidos, pode ser concedido acesso do nodo de submissão 16 ao nodo de processamento 18 sem especificar parâmetros de acesso, como indicado pela seta 224. É então fornecido acesso do nodo de submissão 16 ao nodo de processamento 18 na etapa 212. Se o identificador e senha na declaração de identificação não são válidos na etapa 220, então é negado acesso do nodo de submissão 16 ao nodo de processamento 18 na etapa 216. Deve ser entendido que conceder acesso ao nodo de processamento 18 com o nodo de submissão 16 fornecendo um identificador e senha válidos pode não ser tão seguro quanto forçar que os parâmetros de acesso sejam estabelecidos pelo representante.

Embora a presente invenção tenha sido descrita com várias configurações, uma grande quantidade de mudanças, variações, alterações, transformações e modificações podem ser sugeridas por alguém especializado na técnica, e é pretendido que a presente invenção englobe tais mudanças, variações, alterações, transformações e modificações como estando

situadas dentro do espírito e escopo das reivindicações anexas.

REIVINDICAÇÕES

1. Sistema de processamento de dados compreendendo:

um nodo de submissão (16) tendo um identificador;

um nodo de processamento (18), o nodo de processamento tendo uma memória (46) operável para armazenar um representante (50, 52) associado com o nodo de submissão (16), o representante (50, 52) especificando uma capacidade de processamento ou uma localização na memória (46) do nodo de processamento (18) acessível pelo nodo de submissão (16), o nodo de processamento (18) operável para receber o identificador do nodo de submissão (16) e para fornecer acesso do nodo de submissão (16) ao nodo de processamento (18) de acordo com o representante (50, 52); e

um nodo remoto (12) acoplado entre o nodo de submissão (16) e o nodo de processamento (18), o nodo remoto (12) sendo operável para receber o identificador do nodo de submissão (16) e para comunicar o identificador com o nodo de processamento (18),

o representante (50, 52) compreendendo:

um representante à distância (50) associado com o nodo de submissão (16), o representante à distância (50) tendo primeiros parâmetros de acesso e um identificador local (102) para o nodo de submissão (16); e

um representante local (52) associado com identificador local (102), o representante local (52) tendo segundos parâmetros de acesso;

CARACTERIZADO pelo fato de que os primeiros parâmetros de acesso, a partir do representante à distância (50), têm precedência sobre os segundos parâmetros de acesso a partir do representante local (52).

2. Sistema, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que o identificador compreende um primeiro identificador associado com o nodo de submissão (16) e um segundo identificador associado com o nodo remoto (12).

3. Sistema, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que o identificador do nodo de submissão (16) é incluído em um processo a ser executado na localização na memória (46) do nodo de processamento (18) especificado pelo representante (50, 52).

4. Sistema de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que o representante compreende:

um diretório de recebimento de arquivo (112, 120) especificando uma localização na memória (46) do nodo de processamento (18) operável para armazenar arquivos para enviar para o nodo de submissão (16); e

um diretório de envio de arquivo (108) especificando uma localização na memória (46) do nodo de

processamento operável para armazenar arquivos recebidos do nodo de submissão (16).

5. Sistema, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que o representante compreende:

uma autorização de recebimento (110) indicando que o nodo de submissão (16) pode receber arquivos armazenados no nodo de processamento (18);

uma autorização de envio (106, 118) indicando que o nodo de submissão (16) pode armazenar arquivos no nodo de processamento (18).

6. Método para proporcionar acesso a um nodo de processamento, compreendendo as etapas de:

comunicar um identificador a partir de um nodo de submissão (16) para um nodo remoto (12);

comunicar o identificador a partir do nodo remoto (12) para o nodo de processamento (18);

recuperar um representante (50, 52) armazenado no nodo de processamento (18) usando o identificador, o representante (50, 52) especificando uma capacidade de processamento ou uma localização em uma memória (46) do nodo de processamento (18) acessível pelo nodo de submissão (16); e

proporcionar o acesso do nodo de submissão (16) ao à capacidade de processamento ou localização na memória do

nodo de processamento (18) de acordo com o representante (50, 52),

o representante (50, 52) compreendendo:

um representante à distância (50) associado com o nodo de submissão (16), o representante à distância (50) tendo primeiros parâmetros de acesso e um identificador local (102) para o nodo de submissão (16); e

um representante local (52) associado com o identificador local (102), o representante local (52) tendo segundos parâmetros de acesso;

CARACTERIZADO pelo fato de que os primeiros parâmetros de acesso, a partir do representante à distância (50), têm precedência sobre os segundos parâmetros de acesso a partir do representante local (52)

7. Método, de acordo com a reivindicação 6, **CARACTERIZADO** pelo fato de que o identificador compreende um primeiro identificador associado com o nodo de submissão (16) e um segundo identificador associado com o nodo remoto (12).

8. Método de acordo com a reivindicação 6, **CARACTERIZADO** pelo fato de que o identificador do nodo de submissão (16) está incluído em um processo a ser executado no nodo de processamento (18).

9. Método de acordo com a reivindicação **CARACTERIZADO** pelo fato de que o representante (50, 52) compreende:

um diretório de recebimento (112, 120) especificando uma localização na memória (46) do nodo de processamento (18) operável para armazenar arquivos para enviar para o nodo de submissão (16); e

um diretório de envio (108) especificando uma localização na memória (46) do nodo de processamento (18) operável para armazenar arquivos recebidos do nodo de submissão (16).

10. Método de acordo com a reivindicação 9, **CARACTERIZADO** pelo fato de que o representante (50, 52) compreende:

uma autorização de recebimento (110) indicando que o nodo de submissão (16) pode receber arquivos armazenados no nodo de processamento (18);

uma autorização de envio (106, 118) indicando que o nodo de submissão (16) pode armazenar arquivos no nodo de processamento (18).

11. Método de acordo com a reivindicação 6 **CARACTERIZADO** pelo fato de compreender:

a recuperação no nodo de processamento (18) de um representante à distância (52) associado com o nodo de submissão (16), o representante à distância (52) tendo uma

pluralidade de primeiros parâmetros de acesso e um identificador local (102) para o nodo de submissão (16);

a recuperação no nodo de processamento (18) de um representante local (50) associado com o identificador local (102), o representante local (50) tendo uma pluralidade de segundos parâmetros de acesso; e

a geração de parâmetros de acesso para o nodo de submissão (16) usando os primeiros parâmetros de acesso a partir do representante à distância (50) e os segundos parâmetros de acesso a partir do representante local (52).

12. Método de acordo com a reivindicação 11, **CARACTERIZADO** pelo fato de que o representante à distância (50) é recuperado em resposta a uma declaração de identificação recebida do nodo de submissão (16).

13. Método de acordo com a reivindicação 11, **CARACTERIZADO** pelo fato de que os parâmetros de acesso compreendem:

um diretório de recebimento (112, 120) especificando uma localização na memória (46) do nodo de processamento (18) operável para armazenar arquivos para enviar para o nodo de submissão (16); e

um diretório de envio (108) especificando uma localização na memória (46) do nodo de processamento (18) operável para armazenar arquivos recebidos do nodo de submissão.

14. Método de acordo com a reivindicação 13, **CARACTERIZADO** pelo fato de que os parâmetros de acesso compreendem:

uma autorização de recebimento (110) indicando que o nodo de submissão (16) pode receber arquivos armazenados no nodo de processamento (18);

uma autorização de envio (108, 118) indicando que o nodo de submissão (16) pode armazenar arquivos no nodo de processamento (18).

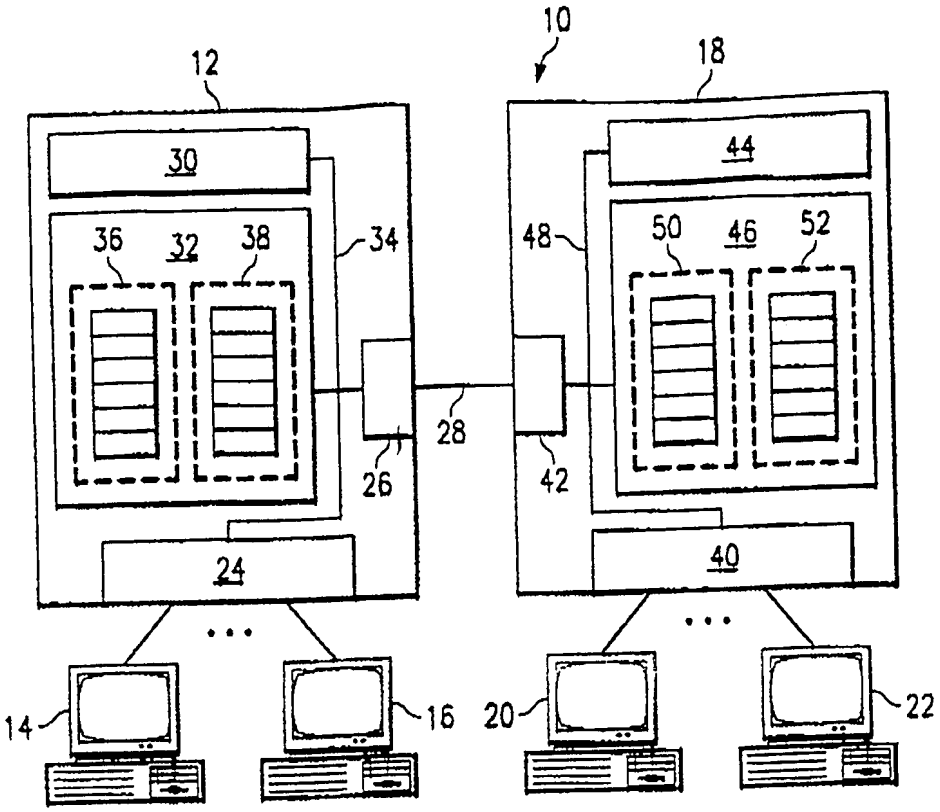
10
12
18
30
44
36
32
38
34
48
50
46
52
28
26
42
24
40
14
16
20
22

FIG. 1

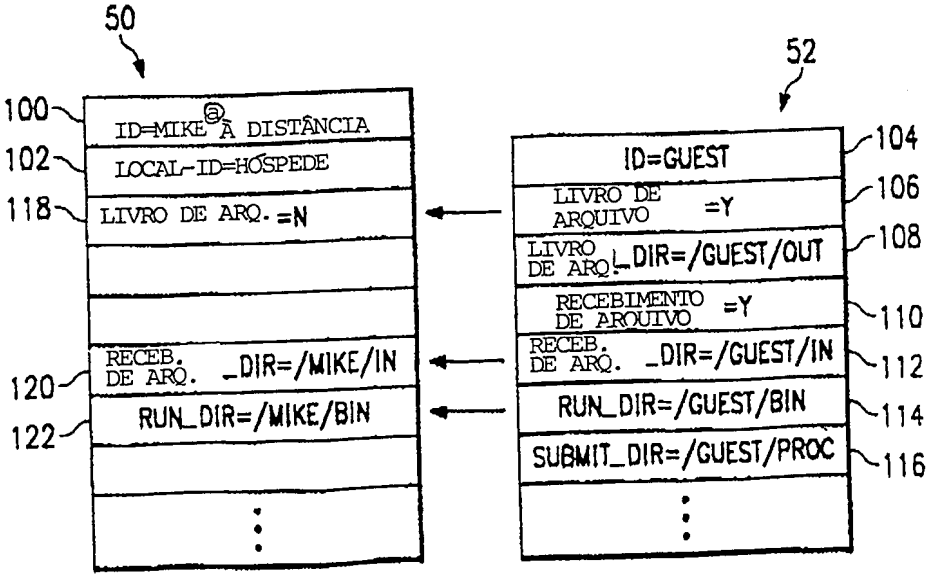
50
52
100
ID=MIKE@A DISTÂNCIA
102
LOCAL-ID=HÓSPEDE
118
LIVRO DE ARQ. =N
120
RECEB. DE ARQ. _DIR=/MIKE/IN
122
RUN_DIR=/MIKE/BIN
ID=GUEST
104
LIVRO DE ARQUIVO =Y
106
LIVRO DE ARQ. _DIR=/GUEST/OUT
108
RECEBIMENTO DE ARQUIVO =Y
110
RECEB. DE ARQ. _DIR=/GUEST/IN
112
RUN_DIR=/GUEST/BIN
114
SUBMIT_DIR=/GUEST/PROC
116

FIG. 2

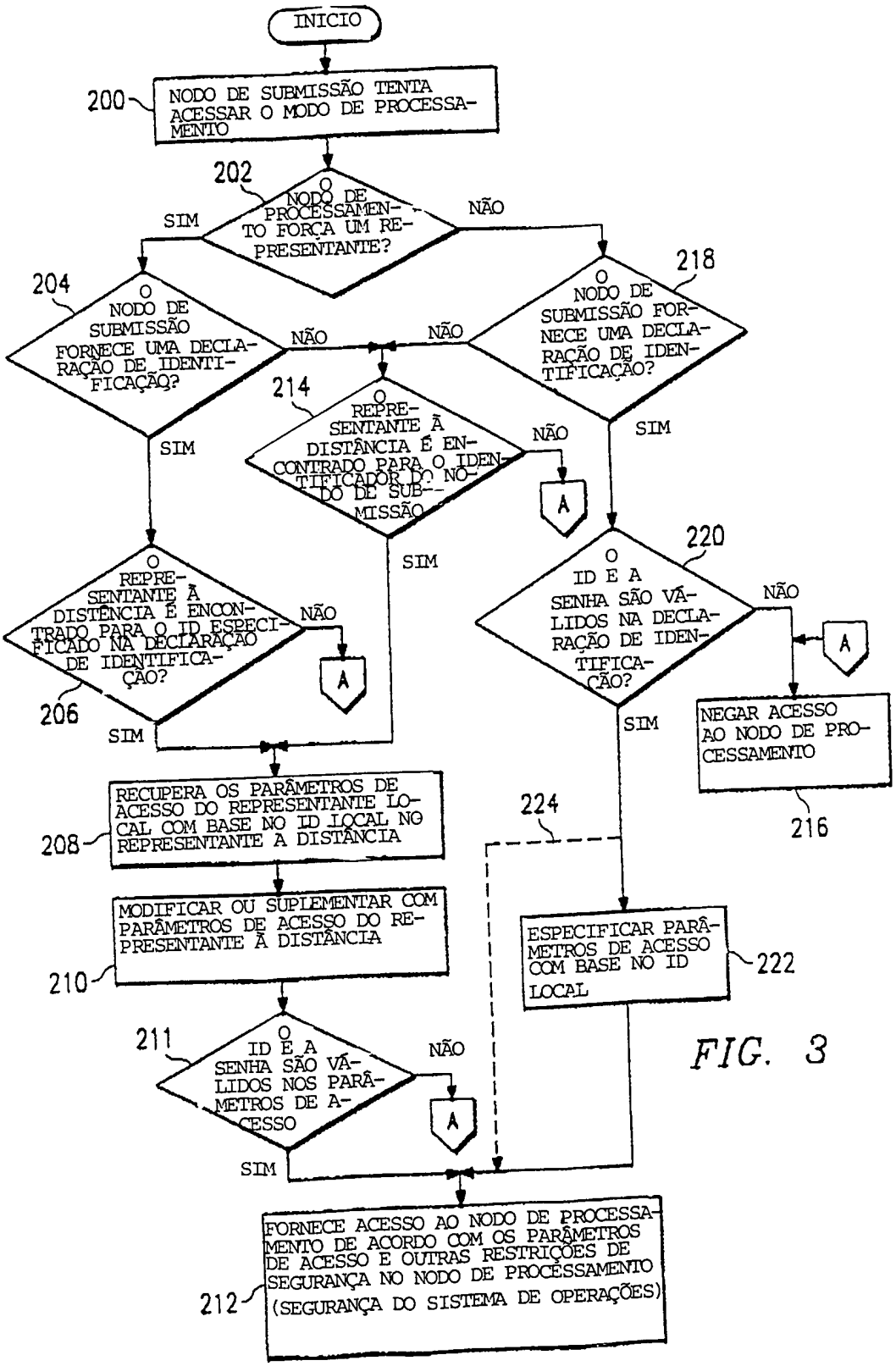
INICIO
200
NODO DE SUBMISSÃO TENTA ACESSAR O MODO DE PROCESSAMENTO
202
O NODO DE PROCESSAMENTO FORÇA UM REPRESENTANTE?
SIM
NÃO
204
O NODO DE SUBMISSÃO FORNECE UMA DECLARAÇÃO DE IDENTIFICAÇÃO?
NÃO
SIM
214
O REPRESENTANTE À DISTÂNCIA É ENCONTRADO PARA O IDENTIFICADOR DO NODO DE SUBMISSÃO
NÃO
SIM
218
O NODO DE SUBMISSÃO FORNECE UMA DECLARAÇÃO DE IDENTIFICAÇÃO?
NÃO
SIM
206
O REPRESENTANTE À DISTÂNCIA É ENCONTRADO PARA O ID ESPECIFICADO NA DECLARAÇÃO DE IDENTIFICAÇÃO?
NÃO
SIM
220
O ID E A SENHA SÃO VÁLIDOS NA DECLARAÇÃO DE IDENTIFICAÇÃO?
NÃO
SIM
A
NEGAR ACESSO AO NODO DE PROCESSAMENTO
216
208
RECUPERA OS PARÂMETROS DE ACESSO DO REPRESENTANTE LOCAL COM BASE NO ID LOCAL NO REPRESENTANTE À DISTÂNCIA
210
MODIFICAR OU SUPLEMENTAR COM PARÂMETROS DE ACESSO DO REPRESENTANTE À DISTÂNCIA
224
222
ESPECIFICAR PARÂMETROS DE ACESSO COM BASE NO ID LOCAL
211
O ID E A SENHA SÃO VÁLIDOS NOS PARÂMETROS DE ACESSO
NÃO
SIM
212
FORNECE ACESSO AO NODO DE PROCESSAMENTO DE ACORDO COM OS PARÂMETROS DE ACESSO E OUTRAS RESTRIÇÕES DE SEGURANÇA NO NODO DE PROCESSAMENTO (SEGURANÇA DO SISTEMA DE OPERAÇÕES)

FIG. 3

RESUMO

"APARELHO E MÉTODO DE SEGURANÇA PARA UM SISTEMA DE PROCESSAMENTO DE DADOS"

Um sistema de processamento de dados (10) inclui nodos de processamento (12, 18) e nodos de submissão (14, 16, 20, 22). Cada nodo de processamento (12, 18) inclui uma lista de representantes à distância (36, 50) e uma lista de representantes locais (38, 52) Os representantes à distância (36, 50) e os representantes locais (38, 52) especificam o acesso às capacidades de armazenagem ou processamento dos nodos de processamento (12, 18) pelos nodos de submissão (14, 16, 20, 22).