República Federativa do Brasil
Ministério da Economia
Instituto Nacional da Propriedade Industrial

(11) PI 1013630-4 B1

(22) Data do Depósito: 23/03/2010

(45) Data de Concessão: 22/04/2020

(54) Título: SISTEMA, E MÉTODO

(51) Int.Cl.: G06F 21/00; H04L 12/22; G06F 15/16.

(30) Prioridade Unionista: 01/04/2009 US 12/416.811.

(73) Titular(es): HONEYWELL INTERNATIONAL INC..

(72) Inventor(es): KEVIN P. STAGGS; PAUL F. MCLAUGHLIN.

(86) Pedido PCT: PCT US2010028218 de 23/03/2010

(87) Publicação PCT: WO 2010/120443 de 21/10/2010

(85) Data do Início da Fase Nacional: 30/09/2011

(57) Resumo: SISTEMA, E MÉTODO Um sistema (100) inclui uma nuvem de computação (108) compreendendo pelo menos uma unidade de armazenamento de dados (112) e pelo menos uma unidade de processamento (110). A nuvem de computação está configurada para se conectar a pelo menos um cliente (102-106) e monitorar o tráfego de pelo menos um cliente. A nuvem de computação ainda está configurada para determinar um modo operacional do cliente, comparar o tráfego monitorado com um padrão de tráfego antecipado associado com o modo operacional e determinar se uma ameaça à segurança é indicada com base na comparação.

SISTEMA, E MÉTODO

CAMPO TÉCNICO

Esta divulgação se refere geralmente a sistemas de computador e, mais especificamente, ao uso da computação em nuvem em aplicações de segurança, e sistemas e métodos relacionados ao uso de computação em nuvem em aplicações de segurança.

FUNDAMENTOS

A computação em nuvem é uma tecnologia emergente na indústria da tecnologia da informação (TI). A computação em nuvem permite o movimento de aplicativos, serviços e dados de computadores de mesa de volta para uma fazenda de servidor principal. A fazenda de servidores pode ser fora das instalações e ser implementada como um serviço. Ao realocar a execução de aplicativos, implantação de serviços e o armazenamento de dados, a computação em nuvem oferece uma maneira sistemática para gerenciar custos de sistemas abertos, centralizar informações e intensificar a robustez e reduzir custos energéticos.

SUMÁRIO

Esta divulgação fornece um sistema e método para usar computação em nuvem em aplicações de segurança.

Em uma primeira modalidade, o sistema inclui uma nuvem de computação compreendendo pelo menos uma unidade de armazenamento de dados e pelo menos uma unidade de processamento. A nuvem de computação é configurada para se

conectar a pelo menos um cliente e monitorar tráfego de pelo menos um cliente. A nuvem de computação é ainda configurada para determinar um modo de operação do cliente, comparar o tráfego monitorado com um padrão de tráfego antecipado associado ao modo operacional e determinar se uma ameaça à segurança é indicada com base na comparação.

Em modalidades particulares, a ameaça à segurança é um ataque contra o cliente por meio de um ataque de negação de serviço (DOS). Em ainda outras modalidades particulares, a ameaça à segurança é um ataque não autorizado ao cliente. Em modalidades adicionais, a nuvem de computação é configurada para relatar uma ameaça à segurança ao cliente.

Em ainda outras modalidades particulares, o modo operacional é selecionado de uma lista de modos operacionais conhecidos e cada modo operacional compreende uma ou mais características em relação ao padrão de tráfego antecipado associado a esse modo operacional.

Ainda em modalidades adicionais, a nuvem de computação é configurada para filtrar dados que chegam ao cliente. Em modalidades ainda adicionais, a filtragem de dados pela nuvem de computação compreende evitar que spam e malware cheguem ao cliente. Em ainda outras modalidades, a filtragem de dados pela nuvem de computação compreende impedir acesso não autorizado ao cliente.

Em uma segunda modalidade, um método inclui definir uma pluralidade de modos operacionais. Cada modo

operacional está associado a pelo menos um padrão de tráfego antecipado de um cliente. O método inclui ainda armazenar a pluralidade de modos operacionais, monitorar tráfego do cliente, determinar o modo operacional do cliente e comparar o tráfego monitorado do cliente com o padrão de tráfego antecipado associado ao modo operacional do cliente.

Em uma terceira modalidade, um sistema inclui uma nuvem de computação compreendendo pelo menos uma unidade de processamento e pelo menos uma unidade de armazenamento de dados. O sistema também inclui um cliente conectado a uma rede através da nuvem de computação. A nuvem de computação é configurada para monitorar o tráfego de rede do cliente, para manter a segurança do cliente.

Outras características técnicas podem ser prontamente aparentes para aqueles versados na técnica a partir das seguintes figuras, descrições e reivindicações.

BREVE DESCRIÇÃO DOS DESENHOS

Para uma compreensão mais completa desta divulgação, referência é feita agora à seguinte descrição, tomada em conjunto com os desenhos em anexo, nos quais:

A FIGURA 1 ilustra um ambiente de computação em nuvem exemplar de acordo com esta divulgação.

A FIGURA 2 ilustra um ambiente de sistema local exemplar de acordo com esta divulgação.

A FIGURA 3 ilustra um sistema de fabricação exemplar

de acordo com esta divulgação.

A FIGURA 4 ilustra um método exemplar de alocar processos e dados de acordo com esta divulgação.

A FIGURA 5 ilustra outro método exemplar de alocar processos e dados de acordo com esta divulgação.

A FIGURA 6 ilustra uma tabela exemplar de condições de tráfego de acordo com esta divulgação.

A FIGURA 7 ilustra um método exemplar de detectar invasões de acordo com esta divulgação;

A FIGURA 8 ilustra um sistema de computador exemplar suportando computação em nuvem de acordo com esta divulgação.

DESCRIÇÃO DETALHADA

As FIGURAS 1 a 8, discutidas abaixo, e as várias modalidades usadas para descrever os princípios da presente invenção neste documento de patente são para ilustração somente e não devem ser interpretadas de forma alguma para limitar o escopo da invenção. Aqueles versados na técnica compreenderão que os princípios da invenção podem ser implementados em qualquer tipo de dispositivo ou sistema devidamente organizado.

A FIGURA 1 ilustra um sistema exemplar 100 de acordo com esta divulgação. A FIGURA 1 mostra os clientes 102, 104 e 106 conectados a uma nuvem de computação 108. A nuvem de computação 108 compreende unidade de processamento 110 e unidade de armazenamento de dados 112, ambas as quais são

acessíveis aos clientes 102, 104 e 106. Um dos aspectos inovadores desta divulgação é a capacidade de projetar uma nuvem flexível e robusta 108 que pode servir uma variedade de ambientes de implantação por meio de uma abordagem híbrida inovadora. Esta abordagem híbrida reconhece tanto o tipo de informação necessária como também a localização de onde essa informação precisa estar. Por exemplo, em um sistema de execução de fabricação (MES) usado no ajuste de uma fábrica automatizada, o sistema deve reconhecer ambos os tipos de informação que precisam ser processados, bem como que informação precisa ser armazenada localmente e que informação pode ser armazenada em uma nuvem de computação.

A nuvem de computação 108 é uma nuvem de computação que é capaz de tanto armazenar informações quanto executar funções de dados em informações. Uma nuvem de computação compreende pelo menos um computador que está acessível de uma localização remota. A nuvem de computação 108 pode compreender uma pluralidade de dispositivos de armazenamento que serão denominados coletivamente como a unidade de armazenamento 112, bem como uma pluralidade de unidades de processamento que serão denominadas coletivamente como a unidade de processamento 110. A nuvem de computação 108 pode compreender hardware que é de custo proibitivo para implantar e manter nos clientes individuais 102, 104 e 106. Além disso, a nuvem de computação 108 pode compreender software que é de custo proibitivo para

instalar, implantar e manter em nuvens de computação individuais. Portanto, a nuvem de computação 108 pode fornecer este hardware e software por meio de conexões seguras para os clientes 102, 104 e 106. Embora haja uma nuvem de computação 108 mostrada na FIGURA 1, é explicitamente entendido que uma pluralidade de nuvens pode ser consistente com esta divulgação.

Os clientes 102, 104 e 106 são computadores individuais, locais de fábricas ou localizações operacionais que estão em comunicação com a nuvem de computação 108. Os clientes 102, 104 e 106 são capazes de acessar tanto a unidade de processamento 110 quanto a unidade de armazenamento 112 que estão localizadas na nuvem de computação 108. Os clientes 102, 104 e 106 são capazes de acessar ambos os processos locais, bem como informações da nuvem de computação 108. Os clientes 102, 104 e 106 podem compreender uma pluralidade de ferramentas de fabricação e sensores para monitorar as ferramentas de fabricação. Estes sensores podem detectar qualquer condição operacional das ferramentas de fabricação incluindo, mas não se limitado a, temperatura, vibração ou outro parâmetro operacional mensurável.

Os clientes 102, 104 e 106 se comunicam com a nuvem de computação 108 por meio de qualquer método seguro ou não seguro, incluindo Hypertext Transfer Protocol Secure (HTTPS) telnet segura, ou File Transfer Protocol Secure

(FTPS). Entende-se que métodos seguros podem ser preferidos em relação a métodos não seguros e que o método particular escolhido dependerá das exigências da função sendo acessada. Esta divulgação não deve ser interpretada como sendo limitada a qualquer protocolo ou método particular de transferir dados.

É assim compreendido que a comunicação entre os clientes 102 a 106 e a nuvem de computação 108 pode ser unidirecional ou bidirecional. Em muitos dos sistemas e métodos divulgados neste documento, a comunicação bidirecional é preferida. A expressão "comunicação unidirecional" se refere à comunicação na qual dados são enviados de um dispositivo de comunicação para um segundo dispositivo de comunicação. O termo "comunicação bidirecional" se refere à comunicação onde dados são enviados e recebidos por dois ou mais dispositivos de comunicação.

Em algumas modalidades, a nuvem de computação 108 pode alavancar uma Arquitetura Orientada a Serviço (SOA) para abstrair consumidores de serviços em nuvem dos próprios serviços de localização. Quando um usuário de nuvem em um determinado cliente invoca uma função, tal como uma função MES, essa função poderá ser executada por componentes MES locais no mesmo cliente ou redirecionados para componentes MES rodando em um servidor na nuvem de computação 108. Este redirecionamento é realizado por um barramento de serviço

que expõe um conjunto de pontos terminais de serviço aos usuários que interagem com estes serviços como se os serviços fossem locais. O barramento de serviço direciona solicitações para esses serviços para os provedores de serviços apropriados, seja localmente ou na nuvem com base em mapeamento configurado. O mapeamento pode ser feito em uma base por serviço, permitindo que uma mistura de serviços locais e baseados em nuvem seja usada. O próprio barramento de serviço pode ser local à planta ou também estar localizado na nuvem. Os sistemas e métodos revelados podem ser projetados para arrendamento múltiplo, de tal forma que muitas empresas possam compartilhar os mesmos recursos de banco de dados físicos, mas manter seus respectivos dados inteiramente privados.

Uma das características inovadoras desta divulgação é o uso de uma abordagem híbrida quando distribuindo armazenamento de dados e processamento de dados entre uma pluralidade de nuvens em uso por um sistema de execução de fabricação. Algumas características dos clientes 102, 104 e 106 podem ser mais bem executadas pela nuvem de computação 108 do que no cliente 102, 104 e 106. Ao determinar que funções podem ser executadas de forma mais eficiente na nuvem de computação 108 do que no cliente local 102, 104 e 106, os recursos computacionais podem ser alocados de tal forma a maximizar o desempenho.

A FIGURA 2 é uma ilustração 200 de um sistema local

202. Cada cliente 102, 104 e 106 compreende um sistema local 202. O sistema local 202 compreende uma unidade de processamento local 208, um armazenamento de dados local 210 e uma entrada/saída de dados local 212. A unidade de processamento local 208 pode compreender ambas as funções em tempo real 204 e as funções em tempo não real 206.

Funções em tempo real são aquelas funções que instruem ou controlam outros dispositivos, incluindo os sistemas mecânicos reais utilizados em uma fábrica. Estas funções em tempo real geralmente sempre devem estar disponíveis e podem ser projetadas para serem não intensivas em recursos. Um exemplo destas funções em tempo real pode incluir a programação de um sistema básico automatizado para executar uma função específica (por exemplo, perfuração em uma substância) por um tempo específico.

Funções em tempo não real podem ser usadas para formar as funções em tempo real. Exemplos de funções em tempo não real são aquelas funções usadas para treinar as funções em tempo real e simulações dos produtos criados pelas funções em tempo não real. Estas funções em tempo não real podem ser intensivas em processador e requer software especializado.

Não apenas podem as funções ser executadas em uma base de tempo real ou tempo não real, os dados podem ser exigidos pelo sistema em uma base de tempo real ou não real. Em uma modalidade, dados que são necessários em uma

base de tempo real serão armazenados localmente no armazenamento de dados local 210, enquanto dados que não são necessários em uma base de tempo real podem ser armazenados na unidade de armazenamento 112 na nuvem de computação 108.

Um dos problemas com a implantação convencional de sistemas MES é que os modelos de simulação mais exatos eram muito caros para implantar nos sistemas locais. Além disso, os modelos de simulação mais precisos tinham requisitos de armazenamento que ultrapassavam o armazenamento disponível do armazenamento de dados local 210. Esta divulgação supera estes problemas por meio de um processo tanto de segregação de dados quanto de segregação de processo. Ao determinar se é exigido que um processo ou dado seja executado em tempo real ou tempo não real, essas funções que podem ser retardadas podem ser colocadas na nuvem de computação 108.

A delimitação entre tempo real e tempo não real é destinada a ser um método exemplar de determinar quais processos e dados devem ser armazenados localmente e que processos e dados devem ser armazenados na nuvem de computação 108. É expressamente entendido que outras delimitações podem ser utilizadas com base em prioridade ou outras características dos dados. Qualquer sistema ou método que delimite processos e armazenamento compartilhados e, em seguida, execute o sistema e método utilizando uma abordagem híbrida em ambas uma nuvem de

computação 108 e um sistema local 202 é explicitamente contemplado por esta divulgação.

Outro exemplo de uma delimitação que pode ser usada para determinar quais dados e quais funções devem ser colocados na nuvem de computação 108 se baseia em se os dados e as funções são de "alto nível" ou "baixo nível". Uma função de alto nível pode incluir uma função que não está diretamente ligada à operação real de uma máquina. Exemplos de funções de alto nível podem incluir programação, reconciliação ou outras funções que podem ser executadas na nuvem de computação 108.

Uma das vantagens da abordagem hibrida divulgada é a intensificação de sistemas de execução de fabricação (MES). Sistemas de execução de fabricação são usados para fornecer instruções ou rotinas para sistemas automatizados básicos. Sistemas automatizados básicos, por sua vez, são utilizados para instruir sistemas diretamente sobre que ações realizar (por exemplo, a operação real de hardware de automação).

Outra vantagem dos sistemas e métodos atualmente divulgados é a capacidade de implementar rapidamente novos serviços ou recursos para uma pluralidade de clientes sem a necessidade de fazer mudanças nos próprios clientes. Quando um novo serviço se torna disponível (por exemplo, a simulação se torna disponível), este serviço pode ser oferecido para melhorar o processo de fabricação em um determinado local sem a necessidade de reprogramação no

local.

Ainda outra vantagem dos sistemas e métodos atualmente divulgados é a capacidade de coleta e análise de dados intensificada. Através da ligação dos clientes 102, 104 e 106 à nuvem de computação 108, os dados podem carregados na nuvem 108 pelos clientes 102, 104 e 106 que representam informações em tempo real relacionadas aos processos de dados. Estas informações podem, por sua vez, ser usadas pela nuvem de computação 108 para uma série de funções, incluindo monitoramento e produção de resultados e identificação de potenciais problemas com o equipamento. Por exemplo, a nuvem pode, em algumas modalidades, aplicar um modelo, tal como um modelo heurístico, para identificar potenciais compromissos na segurança da rede. Estes compromissos para a segurança da rede incluem tanto ataques originados de fora da rede, bem como violações à segurança da rede que se originam de dentro da rede.

A FIGURA 3 é uma modalidade exemplar 300 de um sistema utilizando um sistema de execução de fabricação 302. Nesta modalidade de exemplo, o sistema de execução de fabricação 302 tanto a nuvem de computação 108 quanto o sistema local 202. O sistema de execução de fabricação 302 é usado para controlar o sistema automatizado básico 304. Entende-se que o sistema de execução de fabricação pode compreender uma pluralidade de sistemas locais e uma pluralidade de nuvens de computação.

A FIGURA 4 é um exemplo de um método 400 de executar a abordagem hibrida atualmente divulgada. Nesta modalidade, um modelo é selecionado para alocar processos e dados entre o ambiente local 202 e a nuvem de computação 108 no bloco 402. No bloco 404, os processos para a nuvem são ajustados e dados são armazenados na nuvem. No bloco 406, os processos para o ambiente local são ajustados e dados são armazenados no ambiente local. No bloco 408, a nuvem de computação 108 é ligada ao ambiente local 202. No bloco 410, os processos de fabricação são realizados.

A FIGURA 5 é um fluxograma 500 ilustrando um método para determinar se um determinado processo vai ser executado no ambiente local 202 ou na nuvem de computação 108 usando a delimitação mencionada acima entre descrição de tempo real e tempo não real. Neste fluxograma 500, um processo a ser executado é identificado no bloco 502. No bloco 504, é feita uma determinação quanto a se o processo é requerido por um processo em tempo real. Se o processo for requerido por um processo em tempo real, ele será executado no ambiente local 202 no bloco 512. Se o processo não for requerido por um processo em tempo real, uma determinação é feita no bloco 506 quanto a se o processo é intensivo em armazenamento no bloco 506. Se o processo for intensivo em armazenamento, o processo será executado na nuvem de computação 108 no bloco 510. Se o processo não for intensivo em armazenamento, é feita uma determinação no

bloco 508 quanto a se o processo é intensivo em processador. Se o processo for intensivo em processador, o processo é executado na nuvem de computação 108 no bloco 510, caso contrário o processo é executado no ambiente local 202 no bloco 512. É expressamente entendido que um método semelhante pode ser aplicado para determinar se o armazenamento de dados deve ser armazenado no ambiente local ou na nuvem de computação 108.

A segurança de sistemas industriais exige capacidades ainda mais vigilantes no sistema de automação contra ataques. Alguns tipos exemplares de ataques incluem ataques de negação de serviço (DOS), ataques com home no meio, proteção contra vírus, e-mails indesejados (tal como SPAM) e infiltração de hackers. Estes ataques podem levar a um sendo comprometido por outro sistema de computador. Outro benefício da presente abordagem híbrida é a capacidade de criar um mecanismo de detecção de invasão com base na presença ou ausência de padrões de tráfego anormais detectados pela nuvem de computação 108 no estado de operação do ambiente local 202.

Um problema com sistemas convencionais de dados e detecção de invasão é o número de falsos positivos que são detectados. Esses falsos positivos são frequentemente o resultado de uma mudança no estado de operação de um ambiente local 202. Por meio da abordagem híbrida divulgada, a nuvem de computação 108 pode ser configurada

para fazer uma determinação da condição de tráfego esperada para um determinado estado e, então, comparar a condição de tráfego esperada com a condição de tráfego real. Esta abordagem híbrida permite, portanto, tanto a detecção de invasões, bem como a prevenção de compromissos com segurança.

A FIGURA 6 ilustra uma tabela de exemplo 600 de condições de tráfego de acordo com esta divulgação. Números inteiros são dados para as condições de tráfego e estas se destinam a ser representativas de uma série de fatores, incluindo a quantidade de largura de banda usada atualmente, o número de endereços de protocolo de internet de destino e do tipo de dados sendo transmitidos (tal como a porta através da qual dados estão sendo transmitidos). Esta modalidade da tabela 600 é apenas para ilustração. Nesta implementação específica, a condição de tráfego 1 se refere a baixo tráfego de dados para qualquer localização. A condição de tráfego 2 se refere à baixa transferência de dados, exceto através de uma conexão FTPS. A condição de tráfego 3 se refere a baixa transferência de dados, exceto através de uma conexão FTPS e uma porta de registro. A condição de tráfego 4 se refere a alta transferência de dados entre a nuvem e o ambiente local. A condição de tráfego 5 se refere a altas transferências de dados. Qualquer outro ou tipos adicionais de condição de tráfego podem ser suportados, tal como tráfego de e-mail, tráfego

de protocolo de transferência de arquivos e tráfego de protocolo de transferência de hipertexto.

Na tabela 600 mostrada na FIGURA 6, uma série de estados são apresentados, incluindo um estado de partida 602, um estado de desligamento 604, um estado de manutenção 606, um estado de operação normal 608 e um estado de instalação 610. Em cada um destes estados, uma condição de tráfego esperada e uma condição de tráfego observada são mostradas. Se a condição de tráfego esperada não for igual à condição de tráfego observada, há uma intrusão provável. Os exemplos mostrados na FIGURA 6 se destinam a ser apenas exemplos.

Os inteiros mostrados na FIGURA 6 podem ser criados com base em um sistema de perfil ponderado possibilitado pela nuvem de computação 108. Por exemplo, durante a partida 602, uma grande quantidade de tráfego de alarme de processo pode ser esperada. A nuvem de computação 108 monitorando a transferência de dados por um ambiente local 202 é capaz, por meio de modelagem inteligente, de determinar se o tráfego sendo enviado é consistente com o tráfego que deve estar presente durante a partida. Desta forma, a nuvem de computação 108 pode minimizar os falsos positivos que podem de outra forma estar presentes. Além disso, a nuvem de computação 108 é capaz de determinar qual tráfego está vindo de um invasor e filtrar o tráfego que está sendo iniciado pelo invasor. A nuvem de computação 108

pode usar qualquer tipo de algoritmo para criar um perfil de tráfego de dados esperado, tal como aqueles baseados em modelos empíricos ou observações de transferências de dados reais.

Além do monitoramento, esta abordagem pode ainda incluir filtragem de determinado tráfego de entrada e de saída (tal como toda a atividade de Internet) e verificação de atividade imprópria, maliciosa e ilegal, bem como bloqueio de todo acesso, menos o acesso apropriado e autorizado. A capacidade de fazer triagem prévia de acesso a segurança no nível da nuvem oferece ainda outra camada de segurança nos sistemas divulgados.

A FIGURA 7 ilustra um método exemplar 700 para detectar intrusões de acordo com esta divulgação. No bloco 702, um modo operacional é determinado. No bloco 704, tráfego de dados é monitorado. No bloco 706, o tráfego monitorado é comparado com o tráfego esperado para o modo operacional. No bloco 708, é feita uma determinação quanto a se uma invasão está presente.

A nuvem de computação 108 e os elementos do ambiente local 202 acima descritos pode ser implementados em qualquer computador de uso geral 800 com potência de processamento, recursos de memória e capacidade de manipulação de rede suficiente para lidar com a carga de trabalho necessária colocada no mesmo. Um computador doméstico de uso pessoal, ligado em rede à nuvem de

computação 108 através de uma rede de área ampla, tal como a Internet, pode ser usado em conjunto com as modalidades divulgadas. O computador doméstico de uso pessoal pode partilhar alguns, ou todos, os elementos da nuvem de computação 108. A FIGURA 8 ilustra um sistema típico de computador adequado para implementar uma ou mais modalidades divulgadas neste documento. O computador de uso geral 800 inclui um processador 812 (que pode ser denominado como uma unidade de processamento central ou CPU), que está em comunicação com dispositivos de memória incluindo armazenamento secundário 802, memória de leitura apenas (ROM) 804, memória de acesso aleatório (RAM) 806, dispositivos de entrada/saída (I/O) 808 e dispositivos de conectividade de rede 810. O processador pode ser implementado como um ou mais chips de CPU.

O armazenamento secundário 802 é tipicamente compreendido de um ou mais drives de discos ou drives de fita e é usado para armazenamento não volátil de dados e como um dispositivo de armazenamento de dados de transbordamento se a RAM 806 não for suficientemente grande para conter todos os dados de trabalho. O armazenamento secundário 802 pode ser usado para armazenar programas que são carregados na RAM 806, quando tais programas são selecionados para execução. A ROM 804 é usada para armazenar instruções e, talvez, dados que são lidos durante a execução do programa. A ROM 804 é um dispositivo de

memória não volátil que tipicamente tem uma capacidade de memória pequena em relação à capacidade de memória maior do armazenamento secundário. A RAM 806 é usada para armazenar dados voláteis e, talvez, armazenar instruções. Acesso a ambas ROM 804 e RAM 806 é tipicamente mais rápido do que ao armazenamento secundário 802.

Os dispositivos I/O 808 podem incluir impressoras, monitores de vídeo, telas de cristal líquido (LCDs), telas sensíveis ao toque, teclados, keypads, comutadores, mostradores, mouse, track balls, reconhecedores de voz, leitores de cartões, leitores de fita de papel ou outros dispositivos de entrada bem conhecidos. Os dispositivos de conectividade de rede 810 pode assumir a forma de modems, bancos de modems, placas Ethernet, barramento serial universal (USB), placas de interface, interfaces seriais, placas token ring, placas de Fiber Distributed Data Interface (FDDI), placas de rede de área local sem fio (WLAN), placas de rádio transceptor, tal como sistema de acesso múltiplo por divisão de código (CDMA), e/ou placas de rádio transceptor de sistema global para comunicações móveis (GSM) e outros dispositivos de rede bem conhecidos. Estes dispositivos de conectividade de rede 810 podem permitir que o processador 812 se comunique com a Internet ou uma ou mais intranets. Com tal conexão de rede, é contemplado que o processador 812 pode receber informações da rede, ou pode enviar informações para a rede no curso da

execução das etapas de método acima descritas. Tais informações, que muitas vezes são representadas como uma sequência de instruções a serem executadas usando o processador 812, podem ser recebidas da e enviadas para a rede, por exemplo, na forma de um sinal de dados de computador incorporado em uma onda portadora.

Tais informações, que podem incluir dados ou instruções a serem executadas usando o processador 812, por exemplo, podem ser recebidas da e enviadas para a rede, por exemplo, na forma de um sinal de banda base de dados de computador ou sinal incorporado em uma onda portadora. O sinal de banda base ou sinal incorporado na onda portadora gerada pelos dispositivos de conectividade de rede 810 pode se propagar na ou sobre a superfície de condutores elétricos, em cabos coaxiais, em guias de onda, em mídia óptica, por exemplo, fibra óptica, ou no ar ou espaço livre. As informações contidas no sinal de banda base ou sinal embutido na onda portadora podem ser ordenadas de acordo com diferentes sequências, como pode ser desejável para processamento ou geração das informações ou transmissão ou recepção das informações. O sinal de banda base ou sinal embutido na onda portadora, ou outros tipos de sinais usados atualmente ou no futuro desenvolvidos, aqui denominados como o meio de transmissão, podem ser gerados de acordo com vários métodos bem conhecidos para um técnico no assunto.

O processador 812 executa instruções, códigos, programas de computador, scripts que ele acessa do disco rígido, disquete, disco óptico (estes vários sistemas à base de disco podem ser todos considerados armazenamento secundário 802), ROM 804, 806 RAM ou os dispositivos de conectividade de rede 810.

Embora mostradas como uma série de etapas, várias etapas das FIGURAS 4 e 5 podem se sobrepor, ocorrer em paralelo, ocorrer em uma ordem diferente ou ocorrer várias vezes. Além disso, observem que estas etapas poderiam ocorrer a qualquer momento adequado, tal como em resposta a um comando de um usuário ou dispositivo ou sistema externo.

Em algumas modalidades, várias funções acima descritas são implementadas ou suportadas por um programa de computador que é formado a partir de código de programa legível por computador e que é incorporado em um meio legível por computador. A frase "código de programa legível por computador" inclui qualquer tipo de código de computador, incluindo código fonte, código objeto e código executável. A expressão "meio legível por computador" inclui qualquer tipo de meio capaz de ser acessado por um computador, tal como memória somente de leitura (ROM), memória de acesso aleatório (RAM), um drive de disco rígido, um disco compacto (CD), um disco de vídeo digital (DVD), ou qualquer outro tipo de memória.

Pode ser vantajoso estabelecer definições de certas

palavras e frases usadas em todo este documento de patente. O "acoplar" e seus derivados se refere a qualquer comunicação direta ou indireta entre dois ou mais elementos, se ou não esses elementos estão em contato físico entre si. Os termos "transmitir", "receber" e "comunicar", bem como seus derivados, englobam tanto a comunicação direta como a indireta. Os termos "incluir" e "compreender", bem como seus derivados, significam inclusão sem limitação. O termo "ou" é inclusivo significando e/ou. As frases "associados a" e "associados aos mesmos", bem como seus derivados podem significar incluir, estar incluído dentro, interligado com, conter, estar contido dentro, conectar a ou com, acoplar a ou com, ser comunicável com, cooperar com, intercalar, justapor, estar próximo a, estar ligado a ou com, ter, ter uma propriedade de, ou semelhantes. O termo "controlador" significa qualquer dispositivo, sistema, ou parte dos mesmos que controla pelo menos uma operação. Um controlador pode ser implementado em hardware, firmware, software ou alguma combinação de pelo menos dois dos mesmos. A funcionalidade associada a qualquer controlador particular pode ser centralizada ou distribuída, quer localmente ou remotamente.

Embora esta divulgação tenha descrito certas modalidades e métodos geralmente associados, alterações e permutações destas modalidades e métodos serão aparentes

para aqueles versados na técnica. Portanto, a descrição acima de modalidades exemplares não define ou restringe esta divulgação. Outras mudanças, substituições e alterações também são possíveis sem se afastar do espírito e do escopo desta divulgação, conforme definido pelas reivindicações seguintes.

- REIVINDICAÇÕES -

1. SISTEMA, caracterizado por compreender:

uma nuvem de computação (108) compreendendo pelo menos uma unidade de armazenamento de dados (112) e pelo menos uma unidade de processamento (110);

em que a nuvem de computação está configurada para se conectar um cliente (102-106) e monitorar o tráfego associado com o cliente, selecionar um modo de operação definindo um estado no qual o cliente está operando a partir de uma lista (600) de modos operacionais conhecidos, identificar uma condição de tráfego do tráfego monitorado, comparar a condição de tráfego identificada do tráfego monitorado com um padrão de tráfego previsto associado com o modo operacional selecionado para formar uma comparação, e determinar se uma ameaça à segurança é indicada com base na comparação,

sendo que a nuvem de computação (108) é configurada para identificar a condição de tráfego do tráfego monitorado com base em um número de fatores incluindo um número de destinação de endereço de protocolo de internete para o tráfego, uma quantidade de banda de rede usada, e portas pelas quais o trafego está sendo transmitido.

2. Sistema, de acordo com a reivindicação 1, caracterizado por a ameaça à segurança compreender um ataque ao cliente através de um ataque de negação de serviço (DOS).

3. Sistema, de acordo com a reivindicação 1, caracterizado por cada modo operacional na lista de modos operacionais conhecidos possuir uma ou mais características em relação ao padrão de tráfego esperado associado a esse modo operacional.

4. Sistema, de acordo com a reivindicação 3, caracterizado por a lista de modos operacionais conhecidos incluir um modo de partida, um modo de desligamento, um modo de manutenção, , um modo de operação normal e um modo de instalação.

5. Sistema, de acordo com a reivindicação 3, caracterizado por uma ou mais características referentes ao padrão de tráfego previsto associado com cada modo operacional inclui a quantidade de banda de rede usada, o número de endereços de protocolo de internete de destinação usados, e as portas pelas quais o dado é transmitido.

6. Sistema, de acordo com a reivindicação 1, caracterizado por em que a nuvem de computação ser configurada para filtrar os dados que chegam ao cliente, a filtragem dos dados pela nuvem de computação compreendendo pelo menos um dos: spam e malware impedindo de atingir o cliente e evitar o acesso não autorizado ao cliente.

7. MÉTODO, caraterizado por compreender:

definir uma pluralidade de modos operacionais, os modos operacionais definindo estados nos quais um cliente (102-106) está apto a operar, em que cada modo de operação

está associado a pelo menos um padrão de tráfego previsto do cliente;

armazenar a pluralidade de modos de operacionais como uma lista de modos operacionais conhecidos;

monitorar o tráfego do cliente;

selecionar um dos modos operacionais do cliente a partir da lista de modos operacionais conhecidos, o modo operacional selecionado definindo um estado no qual o cliente está operando,

identificar uma condição de tráfego do tráfego monitorado; e

comparar a condição de tráfego identificada do tráfego monitorado do cliente com o padrão de tráfego previsto associados com o modo operacional do cliente selecionado,

sendo que identificar a condição de tráfego do tráfego monitorado do cliente compreende:

identificar a condição de tráfego do tráfego monitorado com base em um número de fatores incluindo um número de destinação de endereço de protocolo de internete para o tráfego, uma quantidade de banda de rede usada, e portas pelas quais o trafego está sendo transmitido.

8. Método, de acordo com a reivindicação 7, caracterizado por compreender ainda:

impedir uma invasão de computadores, filtrando os dados de tráfego com base na comparação.

9. Método, de acordo com a reivindicação 7, caracterizado por o método ser realizado por uma nuvem de computação (108), e na qual o cliente controla pelo menos uma ferramenta de automação industrial.

10. Método, de acordo com a reivindicação 7, caracterizado por monitorar o tráfego do cliente compreender monitorar pelo menos dois tipos de tráfego, os tipos de tráfego que incluem um arquivo de transferência tipo de tráfego de protocolo e um tipo de tráfego de e-mail.

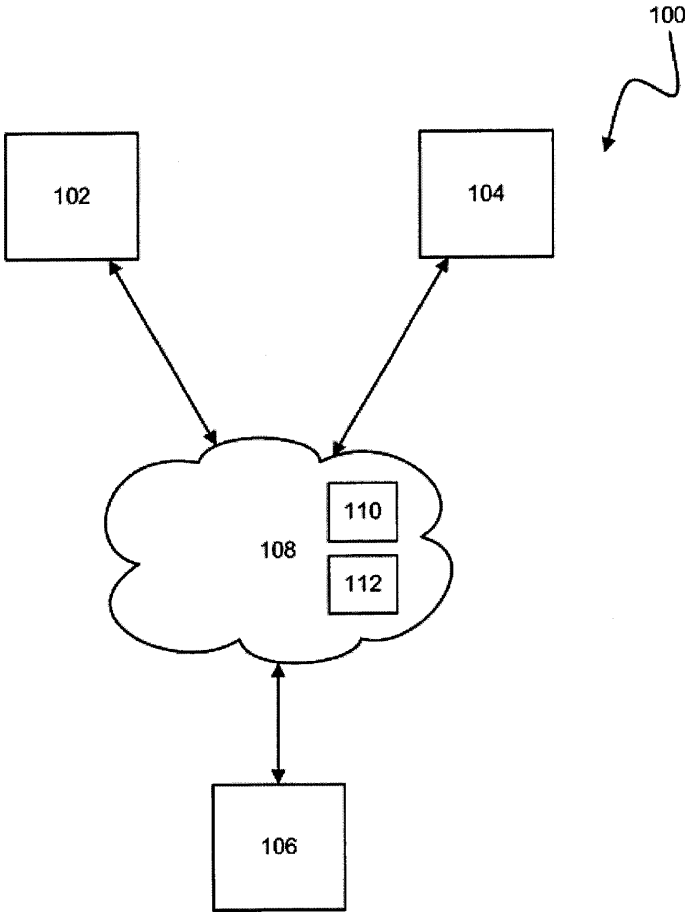

FIG. 1

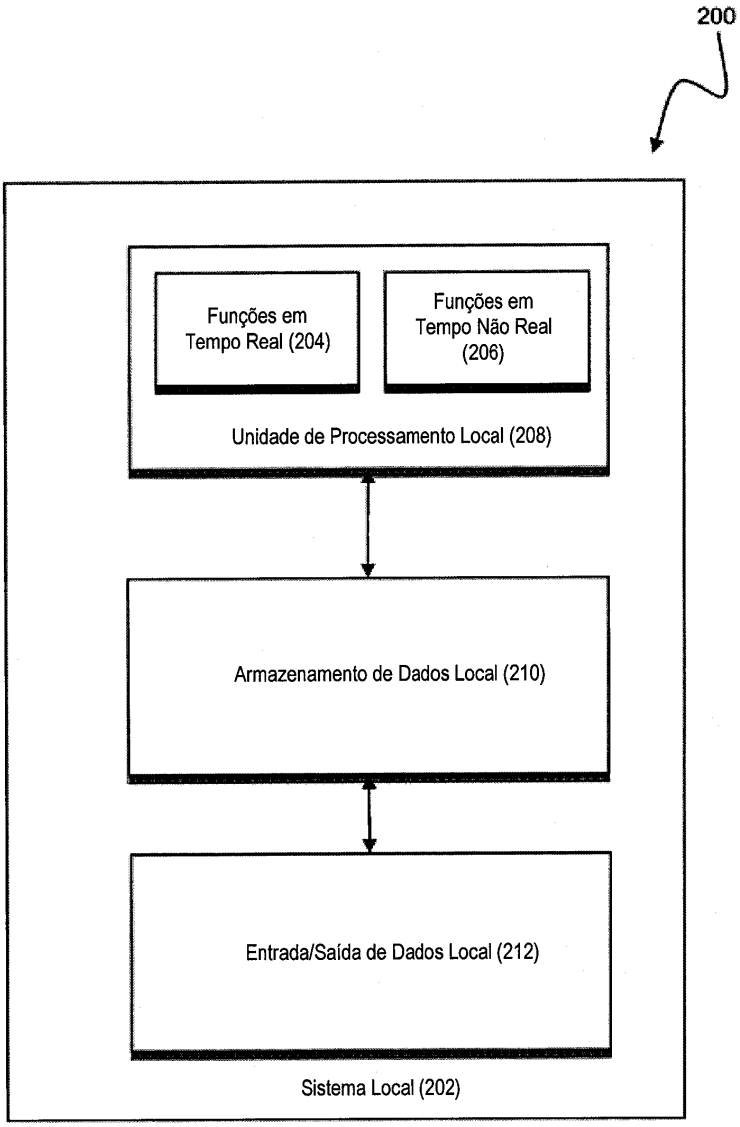
200
Funções em Tempo Real (204)
Funções em Tempo Não Real (206)
Unidade de Processamento Local (208)
Armazenamento de Dados Local (210)
Entrada/Saída de Dados Local (212)
Sistema Local (202)

FIG. 2

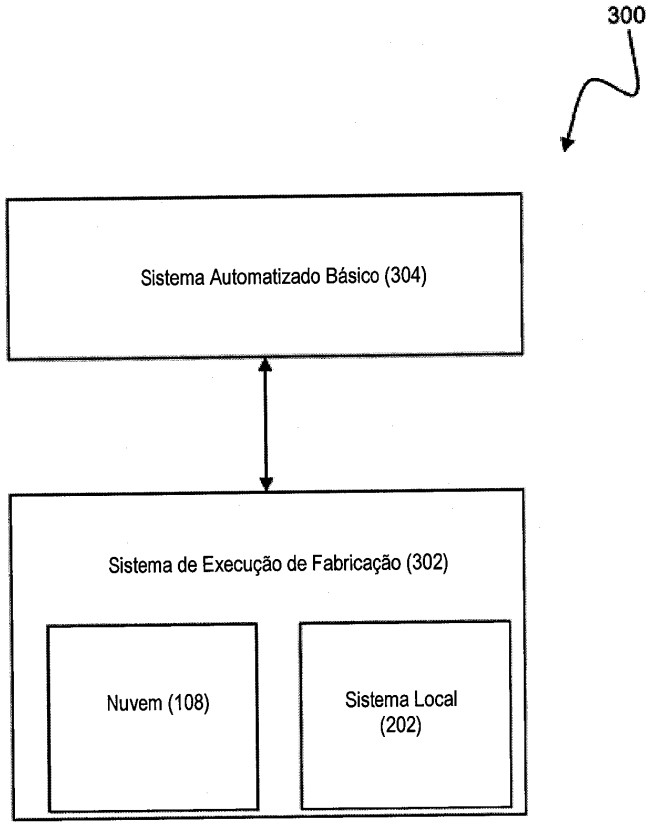
300
Sistema Automatizado Básico (304)
Sistema de Execução de Fabricação (302)
Nuvem (108)
Sistema Local (202)

FIG. 3

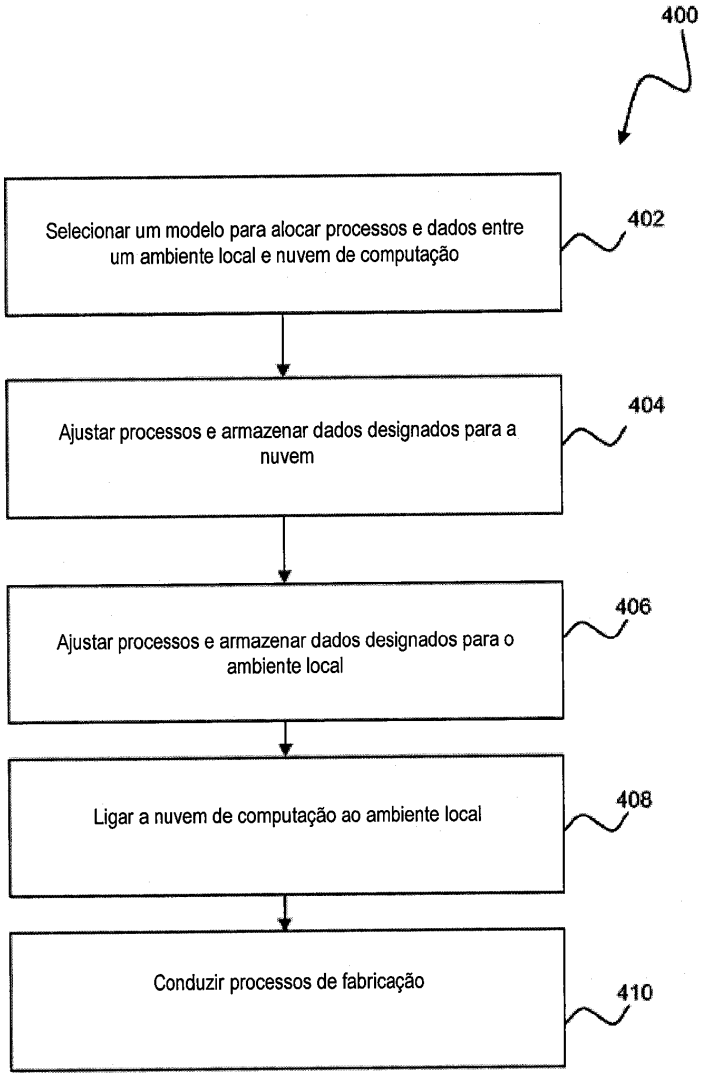
400
Selecionar um modelo para alocar processos e dados entre um ambiente local e nuvem de computação
402
Ajustar processos e armazenar dados designados para a nuvem
404
Ajustar processos e armazenar dados designados para o ambiente local
406
Ligar a nuvem de computação ao ambiente local
408
Conduzir processos de fabricação
410

FIG. 4

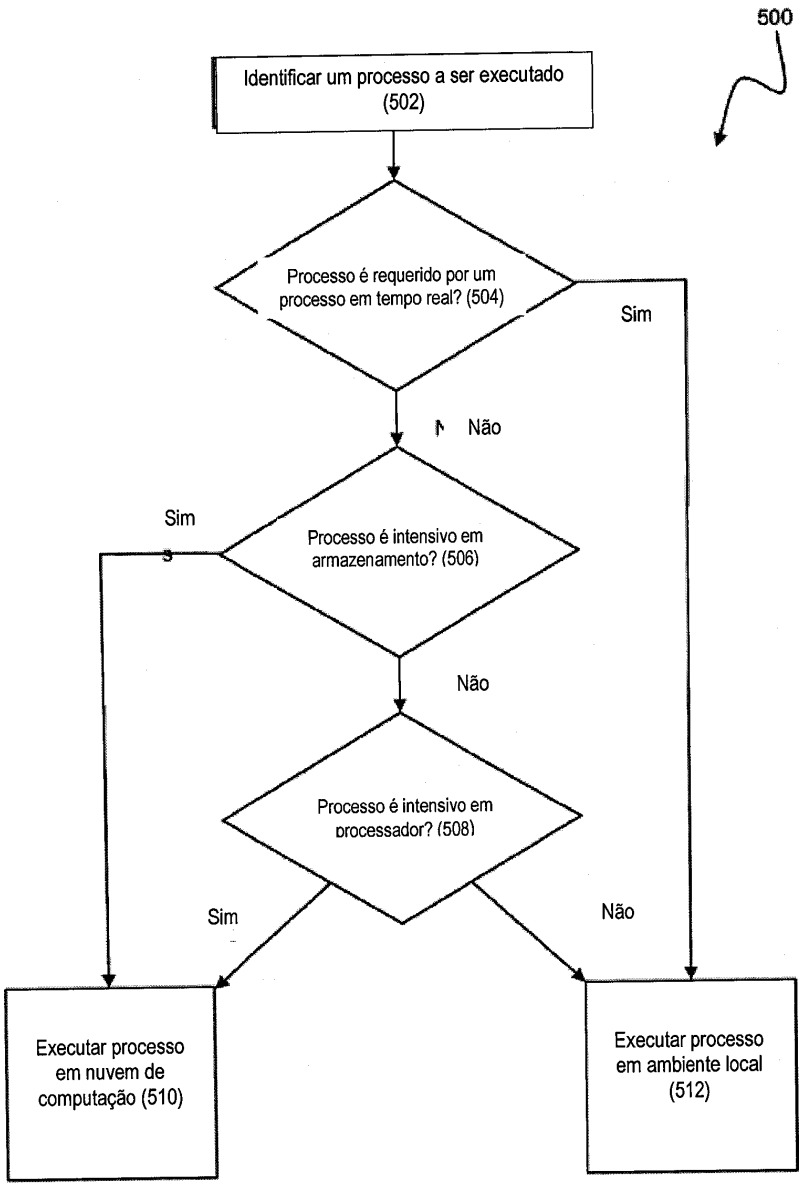
500
Identificar um processo a ser executado (502)
Processo é requerido por um processo em tempo real? (504)
Sim
Não
Sim
Processo é intensivo em armazenamento? (506)
Não
Processo é intensivo em processador? (508)
Sim
Não
Executar processo em nuvem de computação (510)
Executar processo em ambiente local (512)

FIG. 5

Estado	Condição de Tráfego Esperada	Condição de Tráfego Observada	Invasão?
Partida (602)	4	4	N
Desligamento (604)	2	2	N
Manutenção (606)	3	5	S
Operação Normal (608)	1	5	S
Instalação (610)	4	4	N

FIG. 6

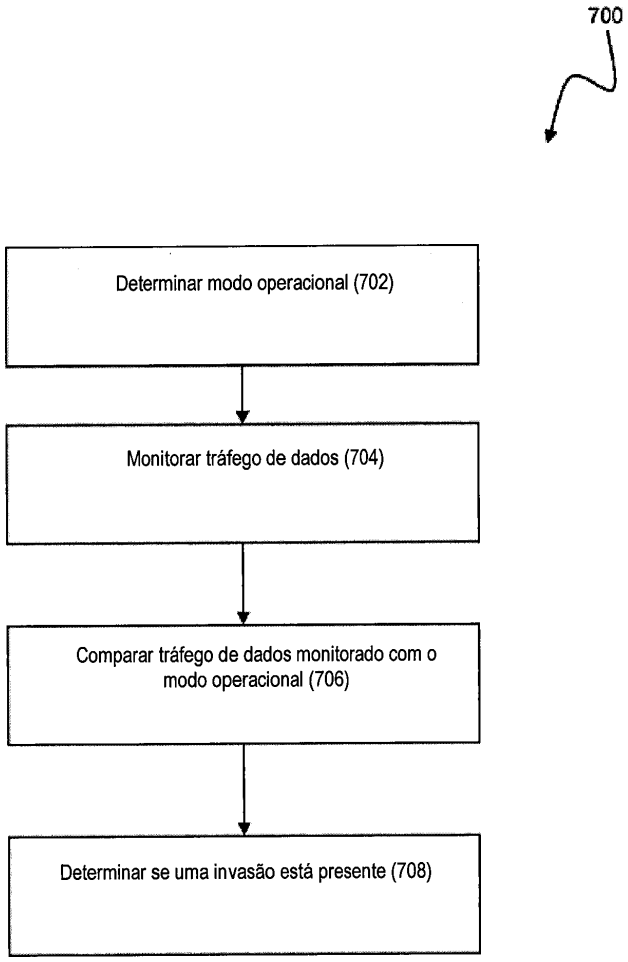
700
Determinar modo operacional (702)
Monitorar tráfego de dados (704)
Comparar tráfego de dados monitorado com o modo operacional (706)
Determinar se uma invasão está presente (708)

FIG. 7

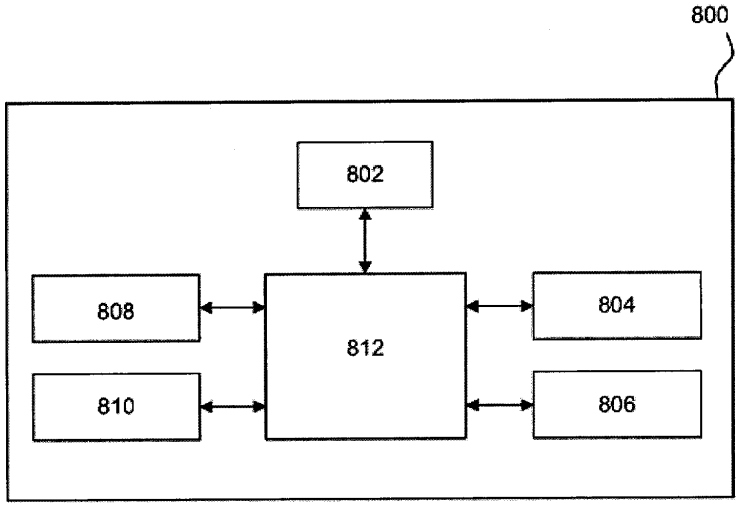

FIG. 8