

DOMANDA DI INVENZIONE NUMERO	102021000021161
Data Deposito	04/08/2021
Data Pubblicazione	04/02/2023

Classifiche IPC

Sezione	Classe	Sottoclasse	Gruppo	Sottogruppo
G	06	F	21	53

Sezione	Classe	Sottoclasse	Gruppo	Sottogruppo
G	06	F	9	455

Sezione	Classe	Sottoclasse	Gruppo	Sottogruppo
G	06	F	9	50

Titolo

SISTEMA DI CONTAINERIZZAZIONE DI WORKSTATION AZIENDALI CON INTERFACCE UTENTE REMOTE A BASSO COSTO
--

Descrizione dell'invenzione avente per titolo:

“SISTEMA DI CONTAINERIZZAZIONE DI WORKSTATION AZIENDALI
CON INTERFACCE UTENTE REMOTE A BASSO COSTO”

a nome: **SIMONCINI MARCO**

a: Fonte Nuova (RM)

Inventore: SIMONCINI Marco

Descrizione

Campo della tecnica

La presente invenzione opera nell'ambito dei sistemi di virtualizzazione di risorse computazionali affrontando le sfide della compatibilità con applicativi grafici utilizzati in numerosi ambiti aziendali.

Arte nota

Una macchina fisica o virtuale, necessitando di un kernel e di un pool di risorse minime assegnate, ha un livello di servizio costante in base all'investimento in termini di risorse assegnate alla macchina. Le soluzioni che permettono di lavorare con un grande numero di operatori comportano un ingente dispendio di risorse connesse alle workstation o agli hypervisor necessari; inoltre, il rischio di crash, fault, downtime relativo all'utilizzo di macchine fisiche o macchine virtuali, soprattutto quando in uso all'utente finale (operatore), è sempre esistente e di notevole impatto sulla produttività. Ad esempio, tutti gli standard relativi agli SLA, Service Level Agreement, stimano una diretta proporzionalità tra il numero di operatori e il numero di incidenti annuali che una struttura risconterà. I tempi di risoluzione degli incidenti costituiscono un doppio costo per la struttura: da un lato il costo di intervento risolutivo, dall'altro il fermo dell'operatore. I container ad oggi sono utilizzati prettamente nelle infrastrutture molto complesse per il deploy di microservizi, si tratta pertanto in gran parte di operazioni che avvengono dietro le quinte e pertanto non rivolte agli operatori finali.

Questa soluzione rappresenta una vera innovazione nel campo della gestione dell'IT di qualunque attività produttiva che comporti l'impiego di molti terminali. Grazie all'utilizzo della tecnologia dei container, piegata dall'inventore alla creazione di pod auto-consistenti, totalmente effimeri nella gestione dei file, raggiungibili da qualunque device e con qualunque sistema operativo anche da sedi remote attraverso l'implementazione all'interno del cluster (i nodi fisici) di terminali Open VPN interni o esterni al cluster, sarà possibile per una qualunque organizzazione abbattere i costi delle workstation e/o dei server, i costi connessi alla gestione dell'IT interno e i tempi di delivery relativi a workstation e server.

Non mancano lavori precedenti, come ad esempio il brevetto US2021019169A1 dove viene presentata un'estensione del kernel come mezzo per containerizzare applicazioni in maniera efficiente. Tuttavia, non è specificata una soluzione per il sistema operativo Windows, né viene presentata una metodologia per sfruttare efficacemente le funzionalità dei container per realizzare un'applicazione grafica con accesso remoto. Nessun riferimento infine è fatto a metodologie per rendere economicamente efficiente l'esperienza di un operatore in azienda con bisogno di accesso ad applicazioni computazionalmente impegnative.

Non v'è dubbio, quindi, che tali soluzioni affrontino soltanto in parte le criticità sin qui esposte.

Descrizione dell'invenzione

Secondo la presente invenzione viene realizzato un sistema di containerizzazione di workstation aziendali con interfacce utente remote a basso costo, che consente un'organizzazione e una distribuzione ottimale dei flussi di lavoro, spesso complessi e dal punto di vista computazionale intensi, agli operatori che lavorano nell'ambito, sfruttando al massimo le risorse hardware in ambiente Cloud. Allo stato attuale qualunque macchina per il computing (client o server) può essere concepita, sia essa fisica o virtuale, solo se munita di un proprio kernel. Per

Kernel si intende il Layer software di gestione e collegamento tra software e hardware che assolve alle diverse funzioni di gestione, come quella delle risorse, degli intervalli, dei processi e di tutte le periferiche. Qualunque macchina per il computing supporta un insieme di servizi necessari al suo funzionamento e alle operazioni per cui la macchina è preposta. A prescindere della consistenza delle risorse ad essa assegnate, variabile in base alla necessità, la singola macchina fisica o virtuale necessita di un insieme di risorse proprie e definite senza le quali non potrebbe funzionare. Ne consegue, che le infrastrutture informatiche attuali, dalle più semplici alle più complesse, possono essere composte da macchine fisiche, macchine virtuali o da una combinazione delle due, tutte munite di un proprio kernel e di un pool di risorse proprie ad esse assegnate. A partire dal 2014 è stata introdotta nel mondo del computing la tecnologia dei container. Per capire meglio l'utilità della presente invenzione è necessario spiegare il concetto di "container". Un container è un'unità astratta di software indipendente e che è eseguibile, in quanto possiede tutto il necessario per eseguire un'applicazione, come: un codice, Runtime, strumenti e librerie di sistema. I container hanno parametri definiti e possono eseguire un programma, un carico di lavoro o un'attività specifica. Una semplice analogia per comprendere i container digitali è pensare alla spedizione dei container fisici. Si può caricare tanta merce in un singolo container ed è possibile caricare tanti container su un'unica nave o suddividerli su più navi. Si possono anche utilizzare container specializzati per carichi di lavoro specifici, allo stesso modo come è possibile utilizzare un container refrigerato per trasportare una specifica tipologia di merce. L'unica limitazione con i container è che dipendono dal loro "kernel" di sistema che li ospita. Un container Linux, ad esempio, può funzionare solo su un host Linux, un container Windows funziona su un host Windows, e così via per altri sistemi operativi. I container consentono agli amministratori di sistema di ottenere una maggiore densità con la loro architettura. È possibile definire ed eseguire più

container, ciascuno personalizzato per un carico di lavoro specifico per ottenere una maggiore efficienza. I container hanno solo il necessario, così da non essere pieni di software superfluo e non sprecare risorse di calcolo sui processi di background. Le aziende stanno scoprendo l'enorme utilità dei container, in quanto sono portatili, coerenti e di facile utilizzo. I reparti IT possono consentire l'integrazione e la fornitura continua con l'agilità e l'automazione che i container offrono, inoltre contribuiscono anche a isolare i carichi di lavoro, contribuendo a solide politiche di sicurezza dei dati. Anche le macchine virtuali sono ambienti di computing indipendenti, astratti dall'hardware, ma a differenza dei container esse richiedono una replica completa di un sistema operativo per poter funzionare. Un vantaggio delle macchine virtuali è che si possono utilizzare per simulare un sistema operativo diverso dal sistema ospite: se la macchina host esegue Windows, è possibile eseguire un sistema operativo Linux in una macchina virtuale e viceversa, inoltre le macchine virtuali consentono un maggiore isolamento e sicurezza dei dati, essendo sistemi di computing ancora più isolati. Tuttavia, poiché quest'ultime sono essenzialmente sistemi indipendenti con il proprio sistema operativo, richiedono tempi di avvio molto più lunghi rispetto ai container e di conseguenza, sono meno efficienti. I container hanno invece, il vantaggio di essere più portatili, poiché un carico di lavoro complesso può essere suddiviso su più container, che possono essere distribuiti ovunque in vari sistemi o infrastrutture cloud. Ad esempio, è possibile distribuire carichi di lavoro su più container nell'hardware in sede e nel servizio di cloud pubblico, gestendo tutto attraverso una singola dashboard di orchestrazione. A motivo di questa portabilità, i container scalano più efficacemente rispetto alle macchine virtuali. Il concetto di container viaggia, infatti, di pari passo con l'utilizzo degli "Orchestratori di Container" come Docker e Kubernetes. Questi strumenti permettono la gestione dei container, la distribuzione dei servizi su più server fisici e la creazione di cluster dedicati al deploy di container. L'orchestrazione è

una metodologia per fornire una visione dall'alto dei container, offrendo visibilità e controllo nei punti d'implementazione dei container e di come vengono allocati i carichi di lavoro su più container. L'orchestrazione è essenziale per implementare più container. Senza orchestrazione, è necessario gestire manualmente ogni singolo container. Una delle funzionalità migliorate grazie all'orchestrazione dei container è la capacità di gestire automaticamente i carichi di lavoro su più nodi di calcolo, con il termine "nodi" si fa riferimento a qualsiasi sistema connesso a una rete, ad esempio, se ci sono cinque server, ma un server avvia un ciclo di manutenzione, l'orchestratore può deviare automaticamente il carico di lavoro nei quattro server rimanenti e bilanciarlo in base a ciò che i nodi rimanenti possono gestire. L'orchestratore può svolgere questa attività senza assistenza umana. Come abbiamo visto, è possibile utilizzare i container per eseguire un compito specifico, un programma o un carico di lavoro, come ad esempio un microservizio, il quale è una funzione specifica di un servizio o un'applicazione più grande. Ad esempio, è possibile utilizzare un container per eseguire una ricerca o una funzione di ricerca su un set di dati, piuttosto che caricare un'intera applicazione di database. Poiché l'operazione funziona all'interno di un ambiente container, viene eseguita più velocemente rispetto a un ambiente di tipo non container, che sia una macchina virtuale o bare metal, con un sistema operativo completo e processi di backup che occupano risorse di calcolo aggiuntive, in questo modo i container rendono più semplice e più veloce la distribuzione e l'utilizzo dei microservizi. Inoltre, all'interno di un ambiente di cloud ibrido, il container diventa l'unità di calcolo, astratta dall'hardware sottostante. Non è necessario preoccuparsi di dove verranno eseguiti i container, poiché è possibile eseguirli ovunque. I container rendono quindi più facile distribuire i carichi di lavoro in un ambiente di cloud ibrido. Ciò viene solitamente gestito tramite la piattaforma di orchestrazione, in modo che gli amministratori abbiano visibilità su dove vengono implementati i

container e quali sono le funzionalità offerte da ogni nodo, tra infrastrutture di cloud pubblico e in sede. Lo scopo per cui è stata realizzata la presente invenzione è quello di rendere i container un'entità utilizzabile da qualsiasi operatore che si trovi ad un terminale sfruttando tutti i vantaggi in termini di affidabilità e di performance che contraddistinguono questa tecnologia. In sostanza, viene consentito l'utilizzo della tecnologia dei container per creare postazioni lavoro da un'infrastruttura hardware centralizzata, minimizzando le risorse necessarie alla singola workstation. Il presente brevetto prevede la presenza di una serie di interfacce utente remote, le quali sono costituite ciascuna da un single-board computer economico, collegato a sua volta a diverse periferiche input-output, la cui tipologia e numero varia in base alle esigenze dell'operatore. Questi single-board computer sono stati progettati per ottimizzare, ad esempio, il rendering grafico, ovvero la "restituzione grafica" "cioè quel processo di generazione di un'immagine a partire da una descrizione matematica di una scena tridimensionale, interpretata da algoritmi che definiscono il colore di ogni punto dell'immagine digitale, su schermi multipli e per un'ampia larghezza di banda. Allo stesso tempo questi single-board computer possiedono delle risorse minime di RAM ed un processore con un'architettura, ridotta al minimo indispensabile, per la visualizzazione dei dati e la comunicazione con il sistema di containerizzazione creato dal presente brevetto, risultando quindi, più economica e semplice. L'invenzione comprende anche un insieme di computer server collegati in rete e con installato un orchestratore di container che consente di gestire l'organizzazione e la distribuzione di container applicativi contenenti le applicazioni desktop utilizzate dagli operatori connessi tramite le suddette interfacce utente remote. Questi container sono creati con un software di containerizzazione che permette di eseguire in modo isolato ed indipendente, un sistema operativo Windows con capacità di accesso grafico remoto, su un

container host con sistema operativo Unix-based, rispettando quindi le specifiche OCI, la Open Container Initiative, che promuove la standardizzazione delle tecnologie container, e ora sotto l'ombrello della Linux Foundation, ha rilasciato la versione 1.0 del proprio runtime per la definizione del ciclo di vita e le specifiche delle immagini che i software containerizzati dovranno avere.

Tutto ciò è reso possibile grazie al livello di personalizzazione possibile nel software open-source KubeVirt che, dopo uno studio approfondito, è stato personalizzato e integrato con driver ed emulatori quali a titolo esemplificativo ma non limitativo QEMU, per permettere di ottenere il livello di integrazione tra hardware e software qui e di seguito descritto. Per ulteriori dettagli di configurazione e di implementazione si rimanda alla documentazione sperimentale e dei software citati.

Vogliamo ora ribadire quanto poter trattare le sessioni di interfaccia con l'utente tramite l'astrazione dei container permette un livello di scalabilità automatica molto più efficace, veloce, semplice e accurata rispetto a quella che si può avere utilizzando classiche macchine virtuali. È chiaro quindi che la ricerca effettuata e le novità qui introdotte sbloccano delle possibilità tecniche importanti nella gestione di applicazioni remote.

Infine, anche se non già oggetto delle sperimentazioni, si propone di utilizzare gli stessi principi, la cui fattibilità è stata testata con sistemi operativi Windows on Unix, possono essere applicati a una collezione di altri sistemi operativi che possono essere eseguiti, in maniera containerizzata, su un qualsiasi altro sistema operativo nativo della macchina.

Il presente sistema, quindi, comprende una serie di container specializzati che garantiscono un alto livello di disponibilità delle applicazioni verso gli operatori, tra i diversi container è prevista la presenza di uno specifico container con la funzione di monitoraggio, il quale consente il recupero delle risorse inutilizzate, e un protocollo di comunicazione di rete personalizzato che permette la

comunicazione tra le applicazioni Windows distribuite al pari di una rete locale LAN, Local Area Network, che corrisponde ad una connessione di dispositivi all'interno di un'area specifica, dove ogni dispositivo viene definito come un nodo della rete ed è collegato al server, anche se non esiste un chiaro limite massimo a ciò che può essere considerato una LAN, questa rete copre tipicamente una piccola area, come un singolo ufficio, un edificio o alcuni edifici all'interno di un'area. Il presente sistema si propone, inoltre, di elaborare, attraverso il software di containerizzazione, specifici container dedicati ai task privi di interazione con l'utente, come ad esempio, container che si occupano sia del bilanciamento del carico, ovvero che hanno il compito di distribuire il carico di elaborazione di uno specifico servizio, ad esempio la fornitura di un sito web (in questo caso prende il nome più specifico bilanciamento carico di rete), tra più server, aumentando in questo modo scalabilità e affidabilità dell'architettura nel suo complesso, sia container che si prefiggono la difesa perimetrale della rete con il software firewall. I cloud e le tecnologie mobile hanno reso obsoleta qualunque strategia di sicurezza basata sulla difesa del perimetro fisico aziendale. Per resistere ad attacchi informatici sempre più sofisticati e mirati, occorre implementare una nuova linea di difesa basata sull'identità digitale e sulla gestione degli accessi, come la IAM l'Identity and Access Management e l'autenticazione a due fattori, anch'essi gestiti da container specifici e indipendenti. L'insieme dei suddetti container vengono collegati ad un file system distribuito condiviso con accessi controllati da un sistema di autorizzazione. Questo file system distribuito è immagazzinato su un sistema di storage condiviso ridondante, secondo protocolli di ridondanza noti, e quindi, accessibile a tutti i container applicativi. Per gestire al meglio la distribuzione dei container il presente sistema è dotato di un pannello di controllo costituito da uno schermo touchscreen, collegato alla rete e provvisto di un software interattivo che è in grado di mostrare i dati di monitoraggio, rilevati dal container specifico di monitoraggio, all'amministratore

dell'infrastruttura. Il presente sistema di containerizzazione consente un sistema di comunicazione altamente efficiente e veloce che abilita a videochiamate, scambio di file, e messaggi tra i dipendenti dell'azienda e tra i dipendenti e i collaboratori esterni. Questi scambi risultano immediati in quanto si basano proprio sulla connessione veloce dei container che fungono da backend per le applicazioni desktop degli operatori, infatti essi sono collocati fisicamente vicini agli operatori e sono, inoltre abilitati ad uno streaming veloce di informazioni per un'esperienza utente migliore rispetto a qualsiasi provider esterno. Per garantire ed innalzare ulteriormente il livello di sicurezza dei dati aziendali, la presente invenzione prevede la presenza di un sistema di partizionamento delle risorse hardware che ha il compito di rendere isolate, a livello hardware, le risorse affidate ai collaboratori esterni. Questo isolamento garantisce un alto livello di cyber-security, tale da rendere inefficaci gli attacchi informatici al software di containerizzazione, creato nel presente brevetto, infatti è previsto che i vari container vadano in esecuzione su macchine fisicamente diverse. Un ulteriore grado di sicurezza viene garantito dalla presenza di una periferica connessa ai single-board computer che ha la funzione di autenticazione dell'hardware, cioè garantisce l'accesso sicuro a file sensibili presenti nel sistema. L'accesso sicuro può avvenire grazie al fatto che questa periferica può essere attivata solo tramite un token hardware, contenuto nel badge aziendale. Il token è un generatore di codici numerici pseudocasuali a intervalli regolari (nell'ordine di poche decine di secondi) secondo un algoritmo che, tra i vari fattori, tiene conto del trascorrere del tempo grazie ad un orologio interno, tale codice, casuale e transitorio, viene combinato con un PIN noto all'utente ed al sistema di autenticazione per generare una password temporanea che può essere usata per effettuare l'autenticazione entro la scadenza dell'intervallo temporale.

I vantaggi offerti dalla presente invenzione sono evidenti alla luce della descrizione fin qui esposta e saranno ancora più chiari grazie alle figure annesse e alla relativa descrizione dettagliata.

Descrizione delle figure

L'invenzione verrà qui di seguito descritta in almeno una forma di realizzazione preferita a titolo esplicativo e non limitativo con l'ausilio delle figure annesse, nelle quali:

- FIGURA 1 mostra gli elementi principali costituenti detto sistema di containerizzazione di workstation aziendali con interfacce utente remote a basso costo, il quale comprende una pluralità di interfacce utente remote 100 caratterizzate a loro volta da single-board computer 101 economici collegati a una pluralità di periferiche input-output 102. In particolare, il sistema comprende una periferica per l'autenticazione hardware 600 connessa a detti single-board computer 101 attivabile tramite token hardware 601 contenuto nel badge aziendale e atta a garantire accesso sicuro a file sensibili presenti nel sistema. L' invenzione è inoltre caratterizzata da una pluralità di computer server 103 che sono collegati in rete 104 e sui quali è installato un orchestratore di container 105 atto a gestire il ciclo di vita di una e, una pluralità di container applicativi 106 che contengono le applicazioni desktop da servire agli operatori connessi tramite dette interfacce utente remote. Al fine di recuperare le risorse inutilizzate, tra detti container applicativi è presente un container specializzato con funzione di monitoraggio 109 connesso ad un pannello di controllo costituito da un ulteriore pannello touchscreen 300 collegato con detta rete 104, che attraverso l'utilizzo di un software interattivo, mostra i dati di monitoraggio rilevati. Inoltre, sono presenti ulteriori container specializzati dedicati ai task privi di interazione con l'utente, creati attraverso un software di containerizzazione 107 che permette di eseguire in modalità isolata, un sistema operativo Windows con capacità di accesso grafico remoto, e dedicati a:

bilanciamento del carico 201, firewall 202, IAM 203 e autenticazione a due fattori 204. Detti container risultano essere collegati a un file system distribuito 205 condiviso con accessi controllati da un sistema di autorizzazione accessibile a tutti i container applicativi e immagazzinato su un sistema di storage condiviso ridondante 206. Infine, la figura mostra un protocollo di comunicazione di rete 110 personalizzato atto a permettere la comunicazione tra le applicazioni Windows distribuite.

- FIGURA 2 illustra invece alcuni moduli integranti detto sistema di containerizzazione di workstation aziendali. In particolare, la presente invenzione al fine di garantire un servizio di interazione efficiente è caratterizzata da un sistema di comunicazione 400 atto ad abilitare videochiamate, scambio di file, e messaggi tra dipendenti dell'azienda e tra dipendenti e collaboratori esterni. L'invenzione, inoltre, comprende un sistema di partizionamento delle risorse hardware 500 atto a rendere isolate, a livello hardware le risorse affidate a collaboratori esterni, e a garantire una sicurezza informatica del sistema. Infine, la figura mostra l'ottimizzazione di detti single-board computer 101 implementati per il rendering grafico su schermi multipli e per un'ampia larghezza di banda comprendendo risorse minime di RAM e processore 700 con architettura ridotta al minimo indispensabile.

Descrizione dettagliata dell'invenzione

La presente invenzione verrà ora illustrata a titolo puramente esemplificativo ma non limitativo o vincolante, ricorrendo alle figure le quali illustrano alcune realizzazioni relativamente al presente concetto inventivo.

Con riferimento alla FIG. 1 sono illustrati le componenti principali della presente invenzione atta a permettere flussi di lavoro complessi e computazionalmente intensi a una pluralità di operatori attraverso l'utilizzo ottimale di risorse hardware in ambiente Cloud. Al fine di consentire ciò il sistema prevede: una pluralità di interfacce utente remote 100 caratterizzate a loro volta da single-

board computer 101 collegati a una pluralità di periferiche input-output 102 in base alle esigenze dell'operatore. In particolare, detti single-board computer 101 sono connessi a una periferica specializzata per l'autenticazione hardware 600 attivabile tramite token hardware 601 contenuto nel badge aziendale e atta a garantire accesso sicuro a file sensibili presenti nel sistema. La figura illustra inoltre, una pluralità di computer server 103 collegati in rete 104 e sui quali è installato un orchestratore di container 105 atto a gestire il ciclo di vita di una e, una pluralità di container applicativi 106 che contengono le applicazioni desktop da servire agli operatori connessi tramite dette interfacce utente remote e atti a fungere da backend per le applicazioni desktop degli operatori, detti container sono infatti collocati vicini fisicamente e abilitati a uno streaming veloce di informazioni per garantire un'esperienza utente migliore rispetto a qualsiasi provider esterno. Detto sistema in particolare prevede, tra detti container applicativi un container specializzato con funzione di monitoraggio 109 atto a recuperare le risorse inutilizzate e connesso ad un pannello di controllo costituito da un ulteriore pannello touchscreen 300 collegato con detta rete 104, che attraverso l'utilizzo di un software interattivo, mostra i dati di monitoraggio rilevati da detto container con funzione di monitoraggio all'amministratore dell'infrastruttura. Il sistema prevede ulteriori container integranti specializzati dedicati a task privi di interazione con l'utente che sono stati creati utilizzando un software di containerizzazione 107 in grado di eseguire in modalità isolata, rispettando quindi le specifiche OCI, un sistema operativo Windows con capacità di accesso grafico remoto, e in particolare sono dedicati a diversi obiettivi quali: il bilanciamento del carico 201, firewall 202, IAM 203 e autenticazione a due fattori 204. In particolare, detti container risultano essere collegati a un file system distribuito 205 condiviso con accessi controllati da un sistema di autorizzazione accessibile a tutti i container applicativi e immagazzinato su un sistema di storage condiviso ridondante 206 secondo protocolli di ridondanza

noti. Infine, l'immagine illustra un protocollo di comunicazione di rete 110 personalizzato atto a permettere l'interazione tra le applicazioni Windows distribuite al pari di una rete locale LAN. Per quanto concerne la figura 2 invece, essa rappresenta le componenti integrative di detto sistema di containerizzazione di workstation aziendali con interfacce utente remote a basso costo. L'invenzione, infatti, prevede un sistema di comunicazione atto ad abilitare videochiamate, scambio di file, e messaggi tra dipendenti dell'azienda e tra dipendenti e collaboratori esterni, detti scambi risultano essere immediati in quanto basati sulla possibilità di sfruttare la connessione veloce tra detti container 106. Al fine di implementare la sicurezza informatica di detto sistema, l'invenzione è caratterizzata da un sistema di partizionamento delle risorse hardware 500 atto a rendere isolate, a livello hardware le risorse affidate a collaboratori esterni, e a garantire una sicurezza informatica del sistema. Detto isolamento consente, infatti, di garantire un livello di cybersecurity superiore rendendo inefficaci possibili attacchi al software di containerizzazione in quanto i container in esecuzione sono collocati su macchine fisicamente diverse. Infine, la figura 2 illustra come detti single-board computer 101 sono implementati per il rendering grafico su schermi multipli e per un'ampia larghezza di banda comprendendo risorse minime di RAM e processore 700 con architettura ridotta al minimo indispensabile per la visualizzazione dei dati in comunicazione con detto sistema di containerizzazione, e quindi di più economica e semplice costruzione.

È infine chiaro che all'invenzione fin qui descritta possono essere apportate modifiche, aggiunte o varianti ovvie per un tecnico del ramo, senza per questo fuoriuscire dall'ambito di tutela che è fornito dalle rivendicazioni annesse.

Rivendicazioni

1. Sistema di containerizzazione di workstation aziendali con interfacce utente remote a basso costo, **caratterizzato dal fatto di** permettere flussi di lavoro complessi e computazionalmente intensi a una pluralità di operatori, con un utilizzo ottimale di risorse hardware in ambiente Cloud; detto sistema comprendendo:
 - A) una pluralità di interfacce utente remote (100) comprendenti a loro volta: un single-board computer (101) economici collegati a una pluralità di periferiche input-output (102) in base alle esigenze dell'operatore;
 - B) una pluralità di computer server (103) collegati in rete (104) e con installato un orchestratore di container (105) atto a gestire il ciclo di vita di una pluralità di container applicativi (106) contenenti le applicazioni desktop da servire agli operatori connessi tramite dette interfacce utente remote;
 - C) detti container essendo creati con un software di containerizzazione (107) che permette di eseguire in modalità isolata, rispettando quindi le specifiche OCI, un sistema operativo Windows con capacità di accesso grafico remoto, su un container host con sistema operativo Unix-based;detto sistema comprendente quindi container specializzati (108) atti a garantire un alto livello di disponibilità delle applicazioni verso gli operatori, in particolare comprendendo almeno un container con funzione di monitoraggio (109) atto a recuperare le risorse inutilizzate, e un protocollo di comunicazione di rete (110) personalizzato atto a permettere la comunicazione tra le applicazioni Windows distribuite al pari di una rete locale LAN.
2. Sistema di containerizzazione di workstation aziendali con interfacce utente

remote a basso costo, secondo la precedente rivendicazione 1, **caratterizzato dal fatto di** comprendere container dedicati ai task privi di interazione con l'utente, creati con detto software di containerizzazione (200) e dedicati a: bilanciamento del carico (201), firewall (202), IAM (203), autenticazione a due fattori (204); detti container essendo inoltre collegati a un file system distribuito (205) condiviso con accessi controllati da un sistema di autorizzazione, detto file system distribuito, accessibile a tutti i container applicativi, essendo immagazzinato su un sistema di storage condiviso ridondante (206), secondo protocolli di ridondanza noti.

3. Sistema di containerizzazione di workstation aziendali con interfacce utente remote a basso costo, secondo una qualsiasi delle precedenti rivendicazioni 1 o 2, **caratterizzato dal fatto di** comprendere un pannello di controllo costituito da un pannello touchscreen (300), collegato con detta rete (104), provvisto di un software interattivo atto a mostrare i dati di monitoraggio rilevati da detto container con funzione di monitoraggio (109) all'amministratore dell'infrastruttura.
4. Sistema di containerizzazione di workstation aziendali con interfacce utente remote a basso costo, secondo una qualsiasi delle precedenti rivendicazioni, **caratterizzato dal fatto di** comprendere un sistema di comunicazione (400) atto ad abilitare videochiamate, scambio di file, e messaggi tra dipendenti dell'azienda e tra dipendenti e collaboratori esterni; detti scambi essendo immediati in quanto basati sulla possibilità di sfruttare la connessione veloce tra detti container (106), atti a fungere da backend per le applicazioni desktop degli operatori, detti container essendo infatti collocati vicini fisicamente e abilitati a uno streaming veloce di informazioni per un'esperienza utente migliore rispetto a qualsiasi provider esterno.
5. Sistema di containerizzazione di workstation aziendali con interfacce utente remote a basso costo, secondo una qualsiasi delle precedenti rivendicazioni,

caratterizzato dal fatto di comprendere un sistema di partizionamento delle risorse hardware (500) atto a rendere isolate, a livello hardware le risorse affidate a collaboratori esterni, detto isolamento atto a garantire un livello di cybersecurity superiore e a rendere inefficaci attacchi al software di containerizzazione sviluppato nella presente invenzione, essendo i container in esecuzione su macchine fisicamente diverse.

6. Sistema di containerizzazione di workstation aziendali con interfacce utente remote a basso costo, secondo una qualsiasi delle precedenti rivendicazioni, **caratterizzato dal fatto di** comprendere una periferica per l'autenticazione hardware (600) connessa a detti single-board computer (101) atta a garantire accesso sicuro a file sensibili presenti nel sistema; detta periferica essendo attivabile tramite token hardware (601) contenuto nel badge aziendale.
7. Sistema di containerizzazione di workstation aziendali con interfacce utente remote a basso costo, secondo una qualsiasi delle precedenti rivendicazioni, **caratterizzato dal fatto che** detti single-board computer (101) sono ottimizzati per il rendering grafico su schermi multipli e per un'ampia larghezza di banda e al contempo comprendendo risorse minime di RAM e processore (700) con architettura ridotta al minimo indispensabile per la visualizzazione dei dati in comunicazione con detto sistema di containerizzazione, e quindi di più economica e semplice costruzione.
8. Sistema di containerizzazione di workstation aziendali con interfacce utente remote a basso costo, secondo una qualsiasi delle precedenti rivendicazioni, **caratterizzato dal fatto che** detti container essendo creati con un software di containerizzazione (107) sono generalizzati a coppie di sistemi operativi host-guest qualsiasi, a titolo esemplificativo ma non limitativo comprendendo anche i sistemi operativi Android-based, BSD-based, macos-based e ios-based.

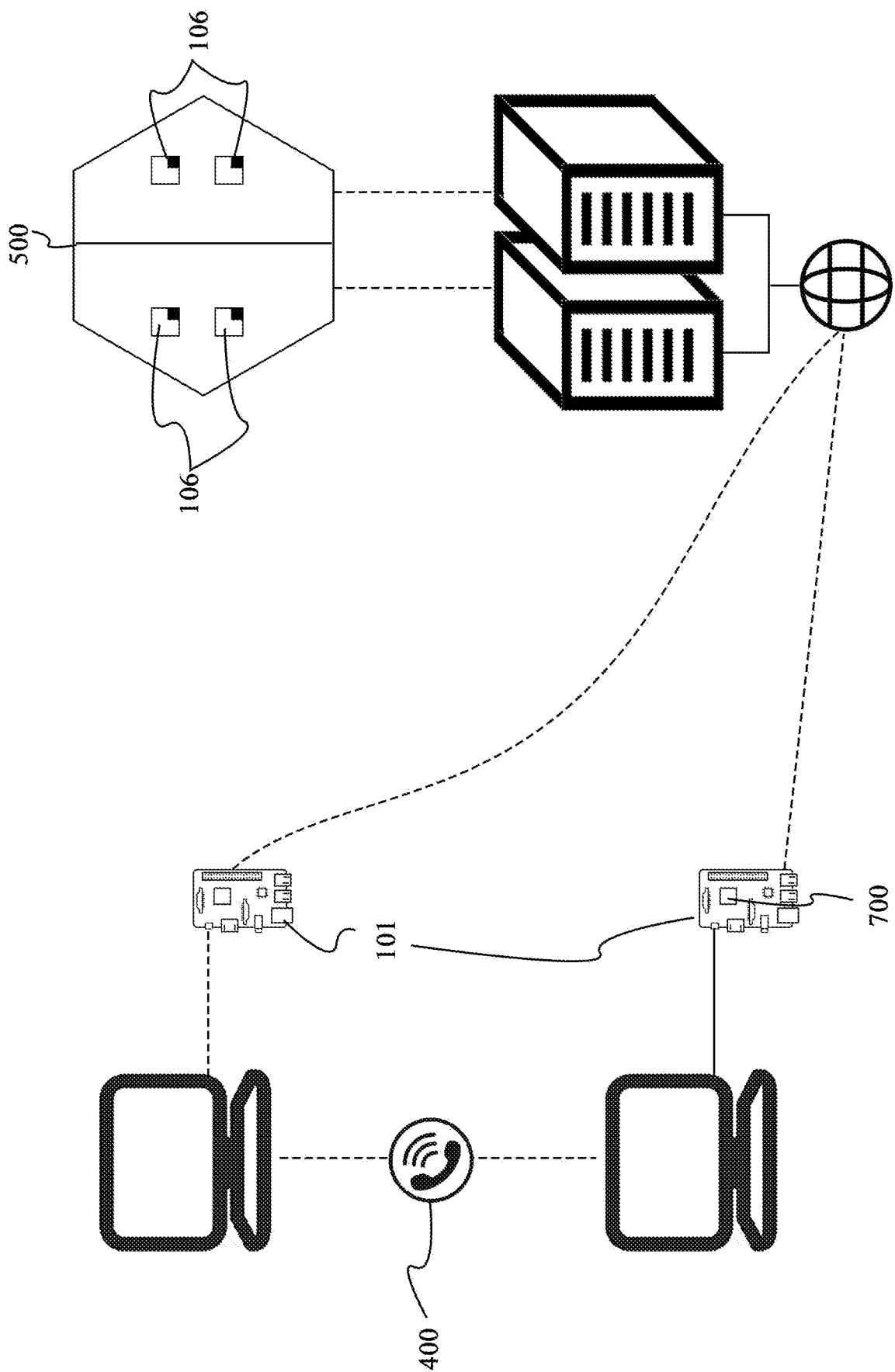


Fig. 2