

MÉTODO Y SISTEMA INDIVIDUAL BASADOS EN ROLES PARA OTORGAR PERMISO A UN USUARIO

ANTECEDENTES

Campo Técnico

[0001] La presente invención está relacionada con un método de administración de permiso de usuario en un sistema de software de administración tal como un sistema ERP, y más particularmente, un método y un sistema individuales basados en roles para otorgar permiso a un usuario.

Arte Relacionado

[0002] El control de acceso basado en roles (RBAC) es uno de los mecanismos de administración para permisos de bases de datos más investigados y maduros en los últimos años. Se considera una alternativa ideal al control de acceso convencional (MAC) y al control de acceso discrecional (DAC). La idea básica del control de acceso basado en roles (RBAC) es para definir diferentes roles de acuerdo con diferentes posiciones funcionales en una vista de organización empresarial, encapsular los permisos de acceso de los recursos de la base de datos en roles y permitir a los usuarios acceder indirectamente a los recursos de la base de datos asignándoles diferentes roles.

[0003] Una gran cantidad de tablas y vistas a menudo están integradas en grandes sistemas de aplicaciones, lo que hace que sea muy complicada administrar y autorizar los recursos de la base de datos. Es extremadamente difícil para el usuario administrar directamente el acceso y la autorización de los recursos de la base de datos. Esto requiere que el usuario tenga una comprensión profunda de la estructura de la base de datos y esté familiarizado con el uso del lenguaje SQL. Además, una vez que la estructura del sistema de la aplicación o los requisitos de seguridad han cambiado, se requiere una gran cantidad de cambios de autorización complejos y engorrosos, y es muy probable que ocurran vulnerabilidades de seguridad causadas por errores de autorizaciones inesperados. Por lo tanto, diseñar un método de administración de permiso simple y efectivo para sistemas de aplicaciones a gran escala se ha convertido en un requisito común para los sistemas y los usuarios del sistema.

[0004] El mecanismo de control de permiso basado en roles puede administrar los

permisos de acceso al sistema de una manera simple y eficiente, lo que reduce en gran medida la carga y el costo de administración de permiso del sistema y hace que la administración de permiso del sistema sea más complicada con especificaciones de administración empresarial del sistema de aplicaciones.

[0005] Sin embargo, el método convencional de administración de permiso basado en roles para un usuario adopta el mecanismo de relación "rol a usuario uno a muchos", y su "rol" es un grupo o una clase por naturaleza, es decir, un rol puede simultáneamente corresponder a o estar relacionado con múltiples usuarios, y el rol es similar a un puesto o una posición o un tipo de trabajo u otros conceptos. El permiso otorgado a un usuario bajo este mecanismo de relación se divide básicamente en las siguientes tres formas: 1, como se muestra en la FIG. 1, el permiso se otorga directamente al usuario, donde la desventaja es que la carga de trabajo es grande y la operación es frecuente e problemática; 2, como se muestra en la FIG. 2, el rol (clase/grupo/puesto/tipo de trabajo) está autorizado (un rol puede estar relacionado con múltiples usuarios) y el usuario obtiene permiso a través del rol; 3, como se muestra en la FIG. 3, los dos métodos de arriba se combinan.

[0006] En las descripciones anteriores, tanto 2 como 3 deben autorizar el rol de la naturaleza de clase/grupo, y el modo de autorización por el rol de la naturaleza de clase/grupo/puesto/ tipo de trabajo tiene las siguientes desventajas: 1. Las operaciones son difíciles cuando cambian los permisos del usuario: En el proceso actual de uso de un sistema, a menudo es necesario ajustar la autoridad del usuario durante el proceso operativo. Por ejemplo, al manejar los cambios del permiso de los empleados, cuando cambia la autoridad de un empleado relacionado con un rol, es inapropiado cambiar los permisos de todo el rol debido a cambios en los permisos del empleado individual, porque el rol también está relacionado con otros empleados cuyas permisos no han cambiado. Por lo tanto, en respuesta a esta situación, se crea un nuevo rol para satisfacer al empleado cuyos permisos se han cambiado o se le otorga permiso directamente al empleado (desconectado del rol) en función de los requisitos del permiso. Los dos métodos de procesamiento de arriba no solo requieren un largo tiempo para la autorización de roles en el caso de una gran cantidad de permisos de roles, sino que también causan errores fácilmente; su uso es engorroso y problemático para el usuario, y también es propenso a errores que resultan en pérdidas para el usuario del sistema.

[0007] 2. Es difícil recordar el permiso específico contenido en el rol durante mucho tiempo: si el rol tiene más funciones de permisos, es difícil recordar los permisos específicos

del rol durante mucho tiempo, y es más difícil recordar las diferencias de permisos entre roles con permisos similares. Si un nuevo usuario necesita estar relacionado, es impracticable determinar exactamente cómo seleccionar un rol para la relación.

[0008] 3. Debido a que cambian los permisos de usuario, se crean más y más roles (si no se crean nuevos roles, esto aumenta en gran medida la autorización directa para el usuario) y es más difícil distinguir las diferencias de los permisos específicos entre roles.

[0009] 4. Cuando un usuario se transfiere desde un puesto, si muchos permisos del usuario transferido se asignarán a otros usuarios, es necesario separar los permisos del usuario transferido y crear roles para relacionarse con otros usuarios. Tal operación no solo es complicada y requiere mucho tiempo, sino que también es propensa a errores.

RESUMEN

Problemas técnicos

[0010] El objetivo de la presente invención es superar las deficiencias del arte anterior y proporcionar un método y un sistema individuales basados en roles para otorgar permiso a un usuario. Un rol solo puede relacionarse con un usuario único durante al mismo tiempo, lo que mejora en gran medida la eficiencia de la administración de permisos de un sistema en uso, hace que la autorización dinámica sea más fácil, más conveniente y más clara y más explícita y mejora la eficiencia y confiabilidad de los ajustes de permisos.

Soluciones a Problemas

Soluciones Técnicas

[0011] El objetivo de la presente invención se logra mediante las siguientes soluciones técnicas: un método individual basado en roles para otorgar permisos a un usuario, que incluye los siguientes pasos secuenciales: S1: crear roles, cada rol es un individuo independiente en lugar de un grupo/clase; S2: autorizando los roles creados en S1 respectivamente; S3: relacionar un usuario con un rol, en el que un rol solo puede relacionarse con un usuario único en el mismo período, y un usuario está relacionado con uno o más roles.

[0012] La autorización de un rol incluye autorización de un formulario, autorización de un menú o autorización de una función.

[0013] Cuando se crea dicho rol, se debe seleccionar un departamento. Una vez que se crea el rol, el rol pertenece al departamento, el rol es único bajo el departamento y el rol se

autoriza de acuerdo con el contenido de trabajo del rol.

[0014] El método individual basado en roles para otorgar permiso a un usuario incluye además un paso de administrar la transferencia entre departamentos, que incluye específicamente: (1) cancelar la relación entre el usuario y el rol en un departamento local; y (2) relacionar al usuario con un rol en un nuevo departamento.

[0015] Dicho usuario solo puede determinar el permiso a través de la relación de dicho usuario con el rol.

[0016] Un método individual basado en roles para otorgar permisos a un usuario, que incluye los siguientes pasos secuenciales: S1: crear roles, cada rol es un individuo independiente en lugar de un grupo/clase; S2: relacionar un usuario con un rol, en el que un rol solo puede relacionarse con un usuario único en el mismo período, y un usuario está relacionado con uno o más roles; S3: autorizando los roles creados en S1 respectivamente.

[0017] La autorización de un rol incluye autorización de un formulario, autorización de un menú o autorización de una función.

[0018] Cuando se crea dicho rol, se debe seleccionar un departamento. Una vez que se crea el rol, el rol pertenece al departamento, el rol es único bajo el departamento y el rol se autoriza de acuerdo con el contenido de trabajo del rol.

[0019] El método individual basado en roles para otorgar permiso a un usuario incluye además un paso de administrar la transferencia entre departamentos, que incluye específicamente: (1) cancelar la relación entre el usuario y el rol en un departamento local; y (2) relacionar al usuario con un rol en un nuevo departamento.

[0020] Dicho usuario solo puede determinar el permiso a través de la relación de este usuario con el rol.

[0021] Un sistema individual basado en roles para otorgar permiso a un usuario, que incluye: una unidad de creación de roles, una unidad de autorización de roles y una unidad de relación usuario-rol; en el que dicha unidad de creación de roles se utiliza para realizar el diseño de los roles de acuerdo con las puestos y crear roles del sistema, cada uno de los cuales es un individuo independiente en lugar de un grupo/clase, dicha unidad de autorización de roles es utilizada para otorgar permisos a roles según el contenido del trabajo de los roles, dicha unidad de relación usuario-rol se utiliza para relacionar a un usuario con un rol y

garantizar que un rol solo pueda relacionarse con un usuario único durante el mismo período, y un usuario está relacionado con uno o más roles.

[0022] Dicho rol del sistema se compone de: un nombre de puesto + un número de puesto.

Efectos beneficiosos de la invención.

Efectos beneficiosos

[0023] (1) El mecanismo de administración de permiso convencional define un rol como grupo, tipo de trabajo, clase, etc. El rol está en una relación de uno a muchos con el usuario. En el proceso actual de uso de un sistema, a menudo es necesario ajustar la autoridad del usuario durante el proceso operativo. Por ejemplo, al manejar los cambios del permiso de los empleados, cuando cambia la autoridad de un empleado relacionado con un rol, es inapropiado cambiar los permisos de todo el rol debido a cambios en los permisos del empleado individual, porque el rol también está relacionado con otros empleados cuyas permisos no han cambiado. Por lo tanto, en respuesta a esta situación, se crea un nuevo rol para satisfacer al empleado cuyos permisos se han cambiado o se le otorga permiso directamente al empleado (desconectado del rol) en función de los requisitos del permiso. Los dos métodos de procesamiento de arriba no solo requieren un largo tiempo para la autorización de roles en el caso de una gran cantidad de permisos de roles, sino que también causan errores fácilmente; su uso es engorroso y problemático para el usuario, y también es propenso a errores que resultan en pérdidas para el usuario del sistema.

[0024] Sin embargo, de acuerdo con el método de la presente aplicación, dado que el rol es un individuo independiente, el permiso del rol puede cambiarse para lograr el objetivo. Aunque la solución de la presente aplicación parece aumentar la carga de trabajo durante la inicialización del sistema, mediante la copia o similar, los roles se pueden crear o autorizar más eficientemente que los roles convencionales de naturaleza del grupo. Debido a que el rol de la naturaleza del grupo no se considera en la comunidad de usuarios relacionada, la solución de la aplicación preventiva hace que los ajustes de permiso sean claro y explícito; especialmente después de usar el sistema por un tiempo (cambios dinámicos de autoridad de usuario/rol), la solución de aplicación preventiva puede mejorar en gran medida la efectividad de la autoridad del sistema utilizada y hacer la autorización dinámica más simple, más conveniente, más clara y más explícita y mejora la eficiencia y la confiabilidad de los ajustes

de permiso.

[0025] (2) El método convencional de autorización de roles basado en grupos es propenso a errores. La solución de la presente aplicación reduce en gran medida la probabilidad de errores de autorización porque en la solución de la presente aplicación, solo es necesario considerar el rol como un individuo independiente, en lugar de considerar la comunidad de múltiples usuarios relacionados con este conjunto de roles como en el método convencional. Incluso si se produce un error de autorización de permiso, el método de corrección de esta aplicación es simple y lleva poco tiempo. Sin embargo, en el caso de un rol convencional de naturaleza grupal, todos los usuarios relacionados con este rol se ven afectados. Incluso si ocurre un error de autorización de permiso, un método de corrección en esta aplicación es simple y toma poco tiempo. Sin embargo, en el caso del rol de tipo de grupo convencional, la comunidad de todos los usuarios relacionados con este rol debe considerarse durante la corrección de errores. La modificación es engorrosa, compleja y propensa a errores cuando el rol tiene muchos puntos de función y, en muchas circunstancias, el problema no puede resolverse a menos que se cree un nuevo rol.

[0026] (3) En el método convencional de permiso de roles basado en grupos, si el rol tiene más puntos de función de permiso, lleva mucho tiempo recordar los permisos específicos del rol y es más difícil recuerde la diferencia en los permisos entre permisos similares. Si es necesario relacionar un nuevo usuario, es imposible determinar exactamente cómo seleccionar un rol para la asociación. En el método de esta aplicación, el rol en sí tiene la naturaleza del número de estación/número de estación y la elección es clara de un vistazo.

[0027] (4) Cuando un usuario se transfiere desde un puesto, si muchos permisos del usuario transferido se asignarán a otros usuarios, es necesario separar los permisos del usuario transferido y crear roles relacionados a otros usuarios. Tal operación no solo es complicada y requiere mucho tiempo, sino que también es propensa a errores.

[0028] La solución de la presente aplicación es la siguiente: el usuario transferido está relacionado con múltiples roles. Cuando el usuario se transfiere de el puesto, su relación con el rol en el departamento original se cancela primero (los roles cancelados se pueden relacionar a otros usuarios), luego el usuario se relaciona con los roles en el nuevo departamento. La operación es simple y no saldrá mal.

[0029] (5) Al crear un rol, se debe seleccionar un departamento. Una vez que se crea el

rol, el departamento no se puede ser reemplazado. El departamento no puede ser reemplazado por las siguientes razones: Razón 1: Debido a que el rol en la presente aplicación es equivalente a un número de estación/número de puesto, el contenido/permisos de trabajo de diferentes números de serie/números de puesto son diferentes. Por ejemplo, los roles de vendedor 1 en el departamento de ventas y desarrollador 1 de departamentos técnicos son dos números de estación/números de puesto completamente diferentes, y sus permisos son diferentes. Razón 2: Si el departamento (departamento de ventas) del vendedor 1 es reemplazado por el departamento técnico y el rol del vendedor 1 permanece sin cambios, hay un rol en el departamento técnico que tiene el permiso del departamento de ventas, lo que puede conducir a confusión de la administración y vulnerabilidades de seguridad.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

DESCRIPCIÓN DE LOS DIBUJOS

[0030] FIG. 1 es un diagrama esquemático de una implementación en la cual un sistema autoriza directamente a un usuario en el arte anterior;

[0031] FIG. 2 es un diagrama esquemático de una implementación en la cual un sistema autoriza un rol de naturaleza del grupo o de la clase en el arte anterior;

[0032] FIG. 3 es un diagrama esquemático de una implementación en la cual un sistema autoriza directamente a un usuario y autoriza un rol de naturaleza del grupo o de la clase en el arte anterior;

[0033] FIG. 4 es un diagrama esquemático de una implementación en la cual un sistema autoriza a un usuario por un rol individual independiente de acuerdo con la presente invención; y

[0034] FIG. 5 es un diagrama de flujo de un método de autorización según la presente invención.

DESCRIPCIÓN DETALLADA

Descripción de las realizaciones

[0035] La solución técnica de la presente invención se describirá con más detalle a continuación con referencia a los dibujos adjuntos, pero el alcance de protección de la presente invención no se limita a lo siguiente.

[0036] [Realización 1] Como se muestra en la FIG. 1, Un método individual basado en

roles para otorgar permiso a un usuario incluye los siguientes pasos secuenciales: S1: crear roles, cada rol es un individuo independiente en lugar de un grupo/clase; S2: autorizando los roles creados en S1 respectivamente; S3: relacionar un usuario con un rol, en el que un rol solo puede relacionarse con un usuario único en el mismo período, y un usuario está relacionado con uno o más roles; una vez que el usuario está relacionado con el rol, el usuario tiene todos los permisos de operación del rol. Además, el usuario solo puede determinar el permiso a través de la relación del usuario con el rol; si se va a modificar el permiso del usuario, el permiso del usuario relacionado con el rol se puede cambiar ajustando los permisos que posee el rol; el usuario no está autorizado directamente, pero sí está autorizado por el rol relacionado con el usuario.

[0037] La relación del rol con el usuario es individual (cuando el rol está relacionado a un usuario, otros usuarios ya no pueden relacionarse con el rol; Si el rol no está relacionado con el usuario, puede estar relacionado con otros usuarios). La relación de un usuario con un rol es de uno a muchos (un usuario puede relacionarse con múltiples roles al mismo tiempo).

[0038] Definición de un rol: Un rol no es la naturaleza de un grupo/clase/categoría/puesto/posición/tipo de trabajo o similar, sino que es de naturaleza no colectiva. El papel tiene su singularidad y es una entidad independiente. Aplicado en una empresa o institución, el rol es equivalente a un número de puesto (el número de puesto aquí no es un puesto, un puesto puede tener múltiples empleados al mismo tiempo, pero un número de puesto es un solo empleado al mismo periodo).

[0039] Por ejemplo, en un sistema empresarial, se pueden crear los siguientes roles: gerente general, subgerente general 1, subgerente general 2, gerente del departamento de ventas de Beijing I, gerente del departamento de ventas de Beijing II, gerente del departamento de ventas de Beijing III, ingeniero de ventas de Shanghai 1, ingeniero de ventas de Shanghai 2, ingeniero de ventas de Shanghai 3, ingeniero de ventas de Shanghai 4, ingeniero de ventas de Shanghai 5, y así sucesivamente. Relación entre usuarios y roles: Si Zhang San, el empleado de la compañía, es el subgerente general 2 de la compañía y es el director del departamento de ventas de Beijing I, Zhang San debe relacionarse con el subgerente general 2 y el gerente del departamento de ventas de Beijing I y Zhang San tienen permiso para ambos roles.

[0040] Autorización de un rol: La autorización del sistema para un rol incluye, entre

otros, autorización de un formulario, autorización de un menú o autorización o de una función. La autorización para la operación del formulario incluye, pero no se limita a, adición, eliminación, inserción y modificación.

[0041] El concepto de roles convencionales es grupo/clase/puesto/posición/tipo de trabajo, y un rol puede corresponder a múltiples usuarios. El concepto de “rol” en la presente aplicación es equivalente al número de puesto/número de estación de trabajo y es similar al rol en el drama de cine y televisión: un rol solo puede desempeñar un papel al mismo tiempo (infancia, juventud, mediana edad, etc.) y un actor puede desempeñar múltiples roles.

[0042] La autorización para un rol incluye, pero no se limita a, la autorización de un formulario, la autorización de un menú o la autorización de una función.

[0043] Cuando se crea dicho rol, se debe seleccionar un departamento. Una vez que se crea el rol, el rol pertenece al departamento, el rol es único bajo el departamento y el rol se autoriza de acuerdo con el contenido de trabajo del rol.

[0044] Si el usuario desea cambiar departamentos, esto implica una transferencia entre departamentos. El proceso de operación específico incluye: (1) cancelar la relación entre el usuario y el rol en el departamento original; y (2) relacionar al usuario con el rol en el nuevo departamento.

[0045] Una vez que se crea el rol, se puede relacionar con un usuario en el proceso de creación del usuario o relacionar el usuario en cualquier momento después de creación del usuario. Una vez que el usuario está relacionado con el rol, la relación con el rol se puede cancelar en cualquier momento y la relación con otros roles también se puede crear en cualquier momento.

[0046] [Realización 2] Un método individual basado en roles para otorgar permiso a un usuario incluye los siguientes pasos secuenciales: S1: crear roles, cada rol es un individuo independiente en lugar de un grupo/clase; S2: relacionar un usuario con un rol, en el que un rol solo puede relacionarse con un usuario único en el mismo período, y un usuario está relacionado con uno o más roles; S3: autorizando los roles creados en S1 respectivamente.

[0047] [Realización 3] Para implementar el método anterior para otorgar permiso, se proporciona un sistema individual basado en roles para otorgar permiso a un usuario, que incluye al menos una unidad de creación de roles, una unidad de autorización de roles y una unidad de relación usuario-rol. Dicha unidad de creación de roles se utiliza para realizar el

diseño de los roles de acuerdo con las puestos y crea roles del sistema, cada uno de los cuales es un individuo independiente en lugar de un grupo/clase, y dicho rol del sistema se compone de: un nombre de puesto + un número de puesto. Por ejemplo: trabajador de la tienda 1, trabajador de la tienda 2, trabajador de la tienda 3, etc. El rol es un individuo independiente equivalente al concepto de número de puesto y un número de estación de trabajo, pero difiere del rol en el sistema convencional de administración de permisos. El concepto de rol en el sistema de administración de permiso convencional es de naturaleza de un grupo o clase, como un puesto, una posición, un tipo de trabajo o similar.

[0048] Dicha unidad de autorización de roles se utiliza para otorgar permiso a roles de acuerdo con el contenido de trabajo de los roles. Dicha unidad de relación usuario-rol se utiliza para relacionar un usuario con un rol y garantizar que un rol solo se pueda relacionar con un usuario único durante el mismo período, y que un usuario esté relacionado con uno o más usuarios. Varios roles.

[0049] [Realización 4] El siguiente ejemplo muestra la relación entre empleados, usuarios y roles después de que el empleado, Zhang San, ingrese a una empresa: 1. Reclutar: una vez que se recluta al empleado, el usuario (empleado) está directamente relacionado con un rol de un número de puesto o número de estación de trabajo correspondiente. Por ejemplo, cuando Zhang San se unió a la empresa (la empresa asigna un usuario a Zhang San) y es responsable de la venta de productos de refrigeración en el área de Beijing bajo el departamento de ventas I (el rol correspondiente es "ingeniero de ventas 5" bajo el departamento de ventas I), el usuario Zhang San selecciona directamente el rol de "ingeniero de ventas 5" y se puede establecer la relación

[0050] 2. Agregar posición: Después de que Zhang San trabajó por un período de tiempo, la compañía le pidió a Zhang San que se hiciera cargo de las ventas de productos de TV en el área de Beijing (el rol correspondiente es "Ingeniero de ventas 8" en el departamento de ventas I) y también es supervisor de departamento de postventa (el rol correspondiente es "supervisor de departamento de postventa 1"). En este caso, dos roles, es decir "ingeniero de ventas 8" en el departamento de ventas I y "supervisor del departamento de postventa 1" en el departamento de postventa, también están relacionados con el usuario Zhang San. En este caso, el empleado Zhang San está relacionado con tres roles: "ingeniero de ventas 5" e "Ingeniero de ventas 8" en el departamento de ventas I y "supervisor de departamento de postventa 1" en el departamento de postventa. Por lo tanto, el usuario Zhang San tiene

permisos de los tres roles.

[0051] 3. Posición reductora: Después de otro período de tiempo, la compañía decide dejar que Zhang San sirva como gerente del departamento de postventa (que corresponde a un rol de “gerente de postventa” en el departamento de postventa) y que ya no otros puestos. En este caso, el usuario Zhang San está relacionado con el rol de "gerente del departamento de postventa" en el departamento de postventa y los tres roles previamente relacionados ("ingeniero de ventas 5" e "ingeniero de ventas 8" en el departamento de ventas I y "supervisor de departamento de postventa 1" en el departamento de ventas) se cancelan. En este caso, el usuario Zhang San solo tiene la autoridad del rol de “gerente de departamento de postventa” en el departamento de postventa.

[0052] 4. Ajustes de permisos de rol (para ajustar los permisos del rol en sí): Si la compañía decide agregar permisos al gerente de departamento de postventa, los permisos solo deben agregarse al rol del gerente del departamento de postventa. Con el aumento de los permisos del rol del gerente del departamento de postventa, también se incrementan los permisos del usuario Zhang San.

[0053] 5. Renunciar: Después de un año, Zhang San renuncia. En este caso, solo es necesario cancelar la relación entre el usuario Zhang San y el rol “gerente del departamento de postventa” en el departamento de postventa.

[0054] Por ejemplo, durante la operación dinámica de la empresa, el reclutamiento y la renuncia del personal a menudo ocurren de manera continua, pero los números de puestos o estación de trabajo rara vez cambian (o incluso permanecen sin cambios dentro de un período de tiempo).

[0055] Método de autorización convencional: en el caso de una gran cantidad de funciones del sistema, la autorización con el rol convencional de grupo/clase implica cargas de trabajo pesadas y engorrosas y es propensa a errores. Peor aún, los errores no pueden detectarse fácilmente en poco tiempo y tienden a causar daños al usuario del sistema.

[0056] En el método de autorización de acuerdo con presente aplicación, los roles de un número de puesto o naturaleza de número de estación de trabajo están autorizados en presente aplicación, y los usuarios están relacionados con los roles para que los permisos del usuario ser determinado. Por lo tanto, los permisos de usuario se controlan simplemente a través de una simple relación usuario-rol. El control de permiso es simple, fácil de operar, claro y

explícito, lo que mejora en gran medida la eficiencia y la confiabilidad de autorización.

[0057] Lo anterior son meramente realizaciones preferidas de la presente invención, y debe entenderse que la presente invención no se limita a las formas descritas aquí, y no debe interpretarse como limitada a otras realizaciones. pero se puede usar en varias otras combinaciones, modificaciones y ambientes. Se pueden realizar modificaciones por las técnicas o el conocimiento de las enseñanzas anteriores o el arte relacionado dentro del alcance de las enseñanzas aquí. Todos los cambios y modificaciones realizados por los expertos en la materia están destinados a estar dentro del alcance de las reivindicaciones adjuntas.

RECLAMACIONES

Lo que se reclama es:

1. Un método individual basado en roles para otorgar permiso a un usuario, que comprende los siguientes pasos secuenciales:

S1: crear roles, cada rol es un individuo independiente en lugar de un grupo/clase;

S2: autorizando los roles creados en S1 respectivamente; y

S3: relacionar un usuario con un rol, en el que un rol solo puede relacionarse con un usuario único en el mismo período, y un usuario está relacionado con uno o más roles.

2. Un método individual basado en roles para otorgar permiso a un usuario de acuerdo con la reclamación 1, en el que, cuando se crea dicho rol, se debe seleccionar un departamento, una vez que se crea dicho rol, dicho rol pertenece a dicho departamento y dicho rol es único en dicho departamento, y dicho rol está autorizado de acuerdo con el contenido del trabajo de dicho rol.

3. Un método individual basado en roles para otorgar permiso a un usuario de acuerdo con la reclamación 2, que comprende además un paso de administración de la transferencia entre departamentos, que comprende específicamente:

(1) cancelar la relación entre dicho usuario y dicho rol en un departamento original; y

(2) relacionar a dicho usuario con un rol en un nuevo departamento.

4. Un método individual basado en roles para otorgar permiso a un usuario de acuerdo con la reclamación 1, en el que dicho usuario puede determinar el permiso solo a través de la relación de dicho usuario con dicho rol.

5. Un método individual basado en roles para otorgar permiso a un usuario, que comprende los siguientes pasos secuenciales:

S1: crear roles, cada rol es un individuo independiente en lugar de un grupo/clase;

S2: relacionar un usuario con un rol, en el que un rol solo puede relacionarse con un usuario único en el mismo período, y un usuario está relacionado con uno o más roles; y

S3: autorizando los roles creados en S1 respectivamente.

6. Un método individual basado en roles para otorgar permiso a un usuario de acuerdo

con la reclamación 5, cuando se crea dicho rol, se debe seleccionar un departamento, una vez que se crea dicho rol, dicho rol pertenece al departamento y dicho rol es único en el departamento, y dicho rol está autorizado de acuerdo con el contenido del trabajo de dicho rol.

7. Un método individual basado en roles para otorgar permiso a un usuario de acuerdo con la reclamación 5, que comprende además un paso de administración de la transferencia entre departamentos, que comprende específicamente:

- (1) cancelar la relación entre dicho usuario y dicho rol en un departamento original; y
- (2) relacionar a dicho usuario con un rol en un nuevo departamento.

8. Un método individual basado en roles para otorgar permiso a un usuario de acuerdo con la reclamación 5, en el que dicho usuario puede determinar el permiso solo a través de la relación de dicho usuario con dicho rol.

9. Un sistema individual basado en roles para otorgar permiso a un usuario, que comprende: una unidad de creación de roles, una unidad de autorización de roles y una unidad de relación usuario-rol, en la cual

dicha unidad de creación de roles se utiliza para realizar el diseño de roles de acuerdo con puestos y crear roles de sistema, cada uno de los cuales es un individuo independiente en lugar de un grupo/clase;

dicha unidad de autorización de rol se utiliza para otorgar permisos a los roles de acuerdo con el contenido de trabajo de los roles; y

Dicha unidad de relación usuario-rol se utiliza para relacionar un usuario con un rol y garantizar que un rol solo se pueda relacionar con un usuario único durante el mismo período, y que un usuario esté relacionado con uno o más usuarios. Varios roles.

10. El sistema individual basado en roles para otorgar permiso a un usuario de acuerdo con la reclamación 9, en el que dicho rol del sistema se compone de: un nombre de puesto + un número de puesto.

RESUMEN

En la presente invención se describe un método un sistema individuales basados en roles para otorgar permiso a un usuario, que incluye los siguientes pasos secuenciales: S1: creando roles, donde cada rol es un individuo independiente en lugar de un grupo o clase; S2: respectivamente autorizando los roles creados en el paso S1; y S3: relacionar un usuario con un rol, donde un rol solo puede estar relacionado con un usuario único en el mismo período, y un usuario puede estar relacionado con uno o más roles. Un rol en la presente invención es un individuo independiente, y es diferente de un rol convencional de una naturaleza de grupo o de clase. Un rol puede estar relacionado con un usuario único en el mismo período de tiempo, lo que mejora en gran medida la eficiencia de la administración de permisos en el uso de un sistema, haciendo que la autorización dinámica sea más simple, más conveniente, más clara y más explícita y mejorando la eficiencia y la confiabilidad del ajuste de permiso.

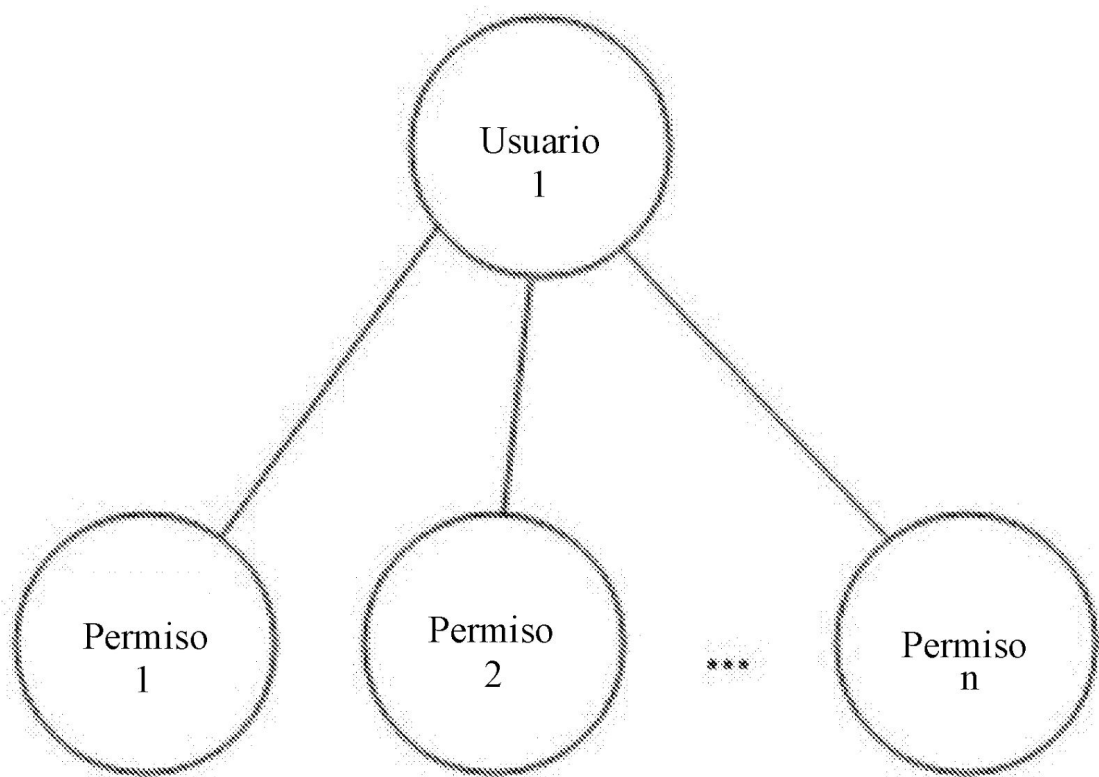


FIG. 1

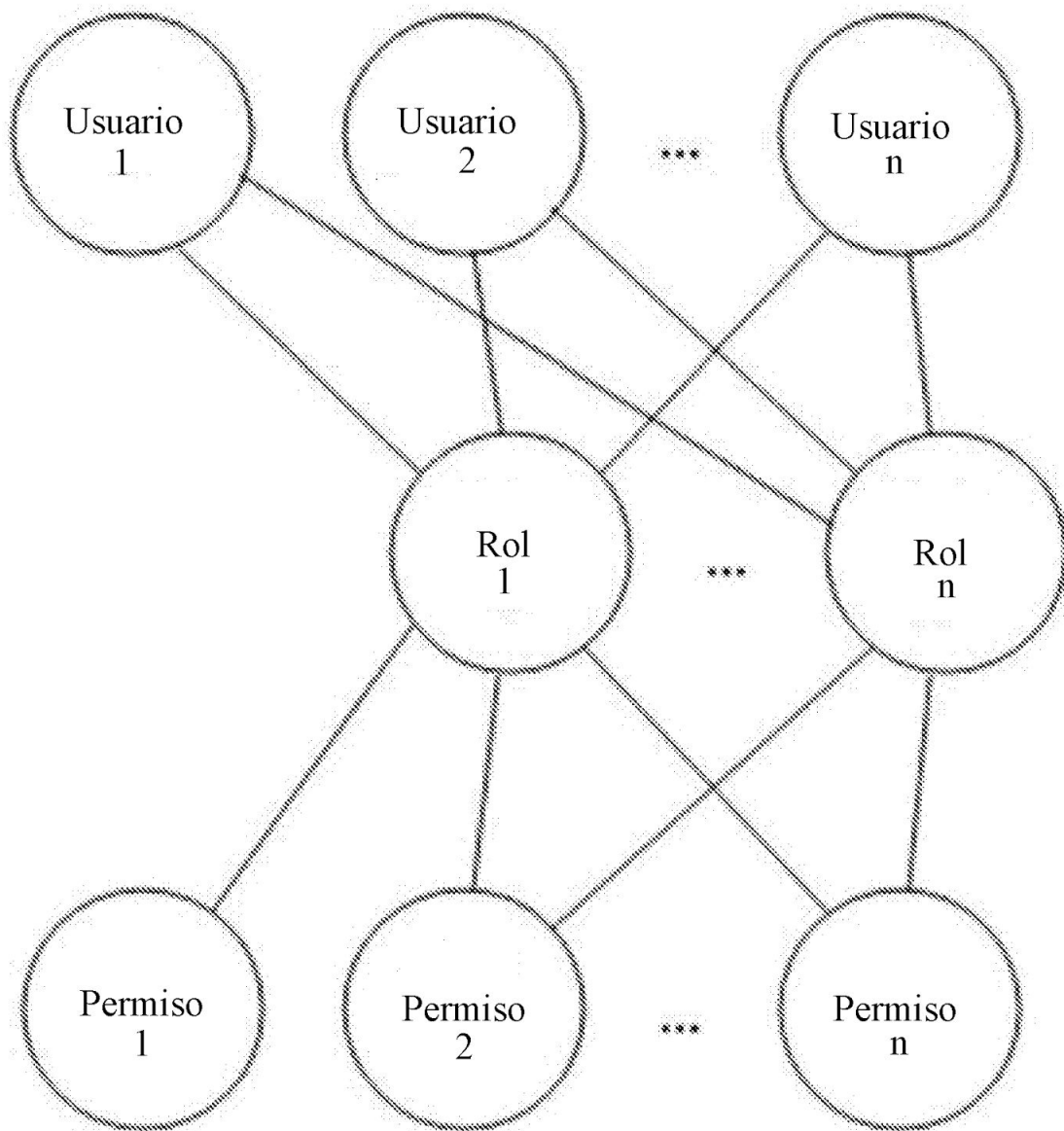


FIG. 2

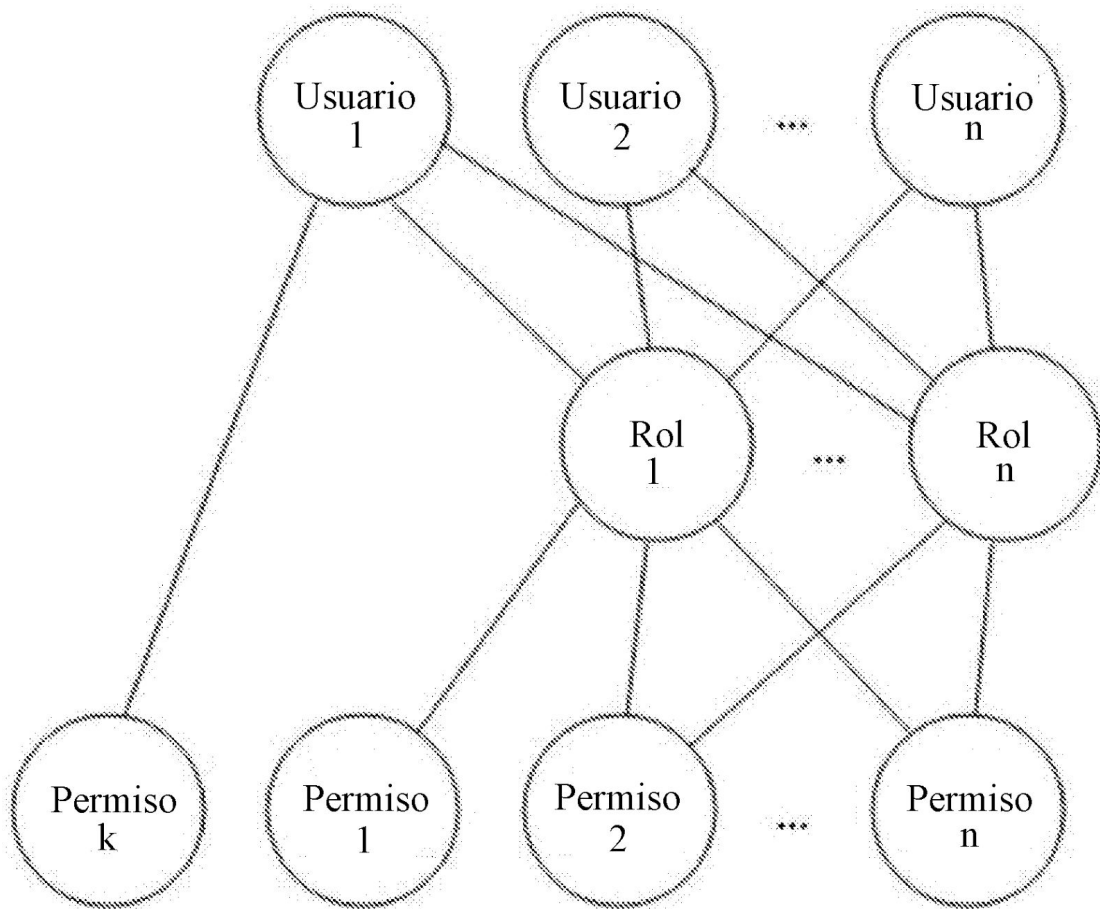


FIG. 3

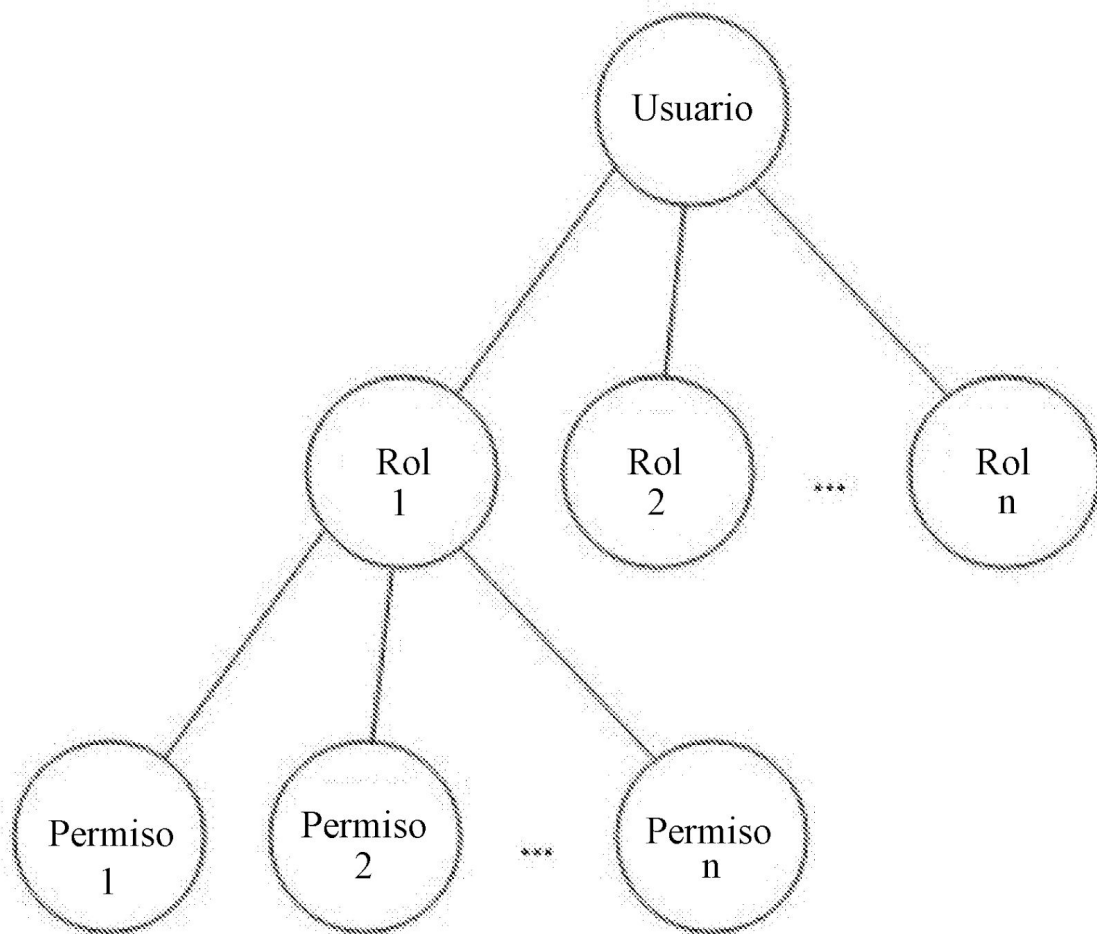


FIG. 4

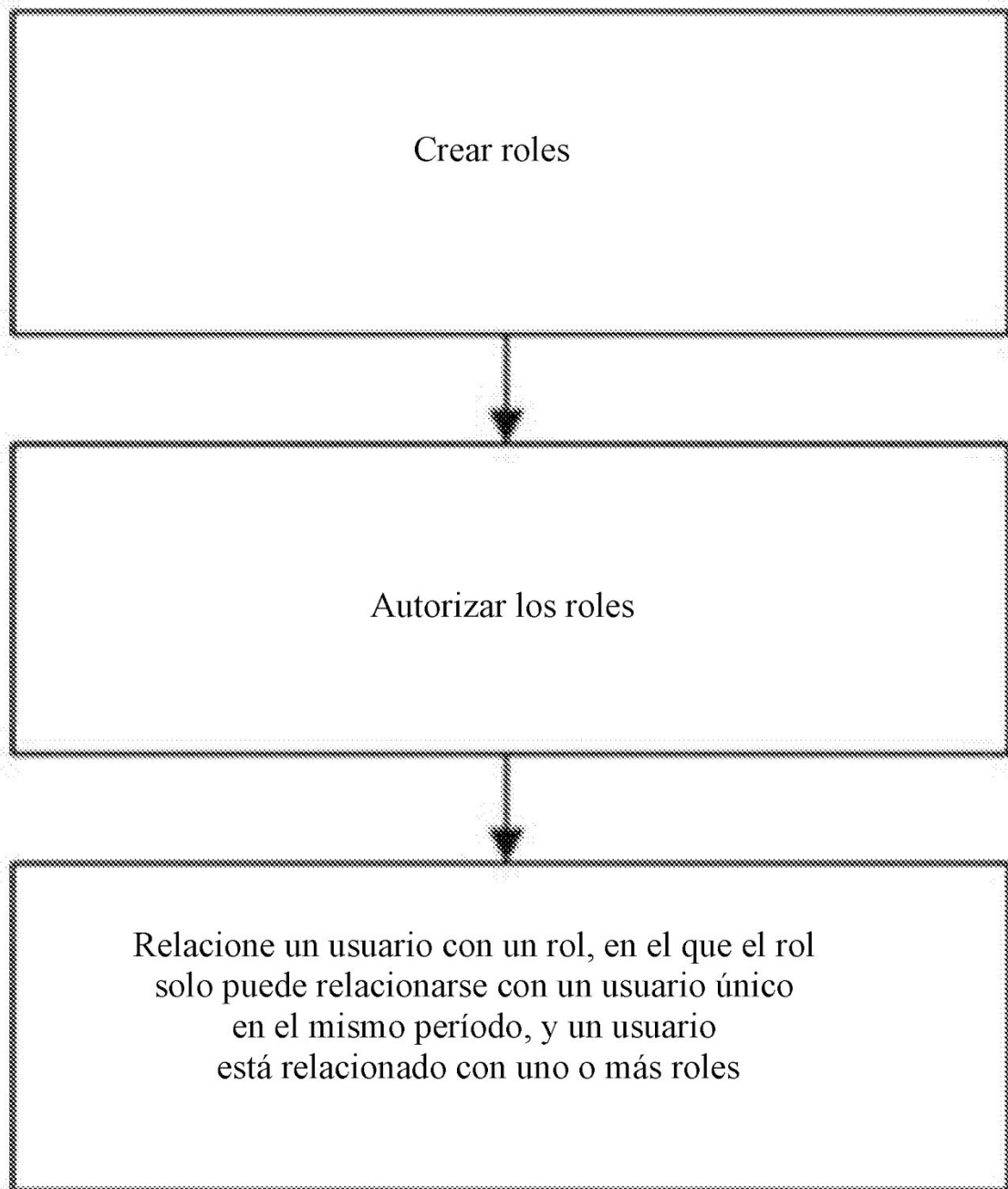


FIG. 5