(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 728 537**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04L 29/08 (2006.01)
H04L 12/58 (2006.01)
H04W 12/12 (2009.01)
G06F 21/56 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **01.10.2014 PCT/GB2014/052967**

(87) Fecha y número de publicación internacional: **09.04.2015 WO15049513**

(96) Fecha de presentación y número de la solicitud europea: **01.10.2014 E 14781934 (6)**

(97) Fecha y número de publicación de la concesión europea: **10.04.2019 EP 3053318**

(54) Título: **Aparato y método de gestión de datos de contenido móvil antimalware**

(30) Prioridad:

04.10.2013 GB 201317607

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
25.10.2019

(73) Titular/es:

GLASSWALL (IP) LIMITED (100.0%)
18A St James's Place
London SW1A 1NH, GB

(72) Inventor/es:

HUTTON, SAM

(74) Agente/Representante:

SÁEZ MAESO, Ana

DESCRIPCIÓN

Aparato y método de gestión de datos de contenido móvil antimalware

Campo de la invención

Esta invención se refiere a redes móviles o inalámbricas en general, y gestión de datos de contenido con base en archivo antimalware en redes móviles o inalámbricas en particular.

Antecedentes de la invención

El malware (tal como virus, troyanos y otros contenidos maliciosos) son cada vez más frecuentes y los enfoques tradicionales para construir firmas para identificar estas amenazas son cada vez más difíciles dada la velocidad a la que están surgiendo nuevas variantes de malware. Estas amenazas no solo se limitan a las redes de ordenadores personales (PC), ya que, con el crecimiento de la implementación del "teléfono inteligente", se ha visto un aumento de malware que atraviesa redes móviles o inalámbricas e infecta dispositivos móviles, por ejemplo, microteléfonos. Un efecto secundario común de estas infecciones de malware y los métodos de protección basados en firmas actuales es el uso del valioso ancho de banda de la red inalámbrica, ya sea como resultado de la infección del virus o como resultado del proceso diario de actualización de firmas.

El documento de Glasswall Solutions Ltd, "How it works", (20121015), web.archive.org, URL:http://web.archive.org/web/20121015004110/http://www.glasswallsolutions.com/how-it-works/, divulga una visión general de alto nivel de cómo funciona el producto Glasswall original.

El documento Glasswall Solutions Ltd, "What it does" (20130116), web.archive.org, URL:http://web.archive.org/web/20130116065146/http://www.glasswallsolutions.com/what-it-does/, divulga una visión general de alto nivel de qué hace el producto Glasswall original.

El documento Glasswall Solutions Ltd, "Where it fits", (20130116), web.archive.org, URL:http://web.archive.org/web/20130116065202/http://www.glasswallsolutions.com/where-it-fits/, divulga una visión general de alto nivel de dónde encaja el producto Glasswall original en los sistemas existentes.

El documento US 2003/196104 A1 describe un proceso de saneamiento de contenido realizado en un motor de transcodificación. El motor de transcodificación puede incluir uno o más patrones, cada patrón identifica contenido malicioso en un documento bien formado. El motor de transcodificación también puede incluir un procesador de anotaciones configurado para anotar porciones del documento bien formado que coinciden con los patrones. Finalmente, el motor de transcodificación puede incluir un procesador de saneamiento de contenido configurado para normalizar las porciones anotadas en un documento transcodificado.

El documento US 2011/090838 A1 divulga técnicas para distribuir contenido en una red de telecomunicaciones móviles, por lo que el contenido se adapta dinámicamente a la calidad del canal del enlace de red que conecta el dispositivo móvil de destino a la red de telecomunicaciones móviles.

Resumen de la invención

Se proporciona un aparato de gestión de datos de contenido móvil antimalware como se establece en la reivindicación 1, un sistema como se establece en la reivindicación 8, y un método de gestión de datos de contenido móvil antimalware como se establece en la reivindicación 9.

La presente invención proporciona un aparato de gestión de datos de contenido móvil antimalware, para uso en gestión de datos de contenido dentro de un archivo electrónico de entrada que contiene datos de contenido para ser enviados a través de una red inalámbrica que comprende por lo menos un dispositivo móvil que es servido por la red inalámbrica, que comprende por lo menos un generador de credenciales para generar de credenciales los datos de contenido incluidos dentro del archivo electrónico de entrada en una representación genérica etiquetada de los datos de contenido, un motor de gestión de contenido para aplicar una política de gestión de contenido predeterminada a la representación genérica etiquetada de los datos de contenido para formar datos de contenido genéricos etiquetados por gestión de contenido, y un validador para crear datos de contenido gestionados por contenido validados al ser dispuestos para asegurar los datos de contenido gestionados por contenido representados en la representación genérica etiquetada gestionada por contenido ajustada a cualesquier limites predefinidos y reglas aplicadas a cada forma de datos de contenido que aparece en los datos de contenido del archivo electrónico de entrada, en el que una salida del validador se acopla operablemente a la red inalámbrica, y se dispone para proporcionar un archivo electrónico de salida sustituto derivado de los datos de contenido gestionados por contenido validados. Los ejemplos pueden utilizar múltiples instancias de la etapa de generador de credenciales.

Los ejemplos pueden incluir adicionalmente por lo menos un filtro para filtrar la representación genérica etiquetada de los datos de contenido para eliminar datos de contenido no referenciados o inalcanzables.

Los ejemplos pueden incluir adicionalmente un regenerador acoplado operablemente al validador y dispuesto para proporcionar el archivo electrónico de salida sustituto derivado de los datos de contenido gestionados por contenido validados al regenerar una nueva instancia de un archivo electrónico en una especificación de tipo de archivo predeterminada para su uso posterior por la red inalámbrica en lugar del archivo electrónico o al emitir los datos de contenido gestionados por contenido validados como una representación genérica etiquetada. Los ejemplos pueden utilizar múltiples instancias del regenerador, cada uno localizado después de una etapa de generación de credenciales inicial, pero antes de una siguiente, posterior etapa de generación de credenciales. Los ejemplos que tienen múltiples instancias de tanto los generadores de credenciales como los regeneradores se pueden mencionar que tienen múltiples pares de generador de credenciales-regenerador. Una especificación de tipo archivo especificado puede ser la misma especificación de tipo de archivo que el archivo electrónico (original) enviado a través de la red inalámbrica, o una especificación de tipo de archivo diferente adecuada para transportar los datos de contenido regenerados, por lo menos en la instancia de regeneración particular involucrada/etapa de procesamiento.

Los ejemplos pueden incluir adicionalmente el motor de gestión de contenido que se configura adicionalmente para normalizar el archivo electrónico de salida sustituto a una versión predeterminada de la especificación de tipo de archivo predeterminada.

En los ejemplos, el aparato de gestión de datos de contenido móvil comprende adicionalmente un motor de ejecución acoplado operablemente al motor de gestión de contenido y dispuesto para proporcionar parámetros de política de gestión de contenido indicativos de, o para uso en aplicar, la política de gestión de contenidos que estará vigente.

En los ejemplos, el aparato de gestión de datos de contenido móvil comprende adicionalmente un monitor de parámetros de red acoplado operablemente al motor de ejecución y dispuesto para proporcionar parámetros de red al motor de ejecución, para su uso en la configuración o modificación de los parámetros de política de gestión de contenido.

En algunos ejemplos, el aparato de gestión de datos de contenido móvil puede comprender adicionalmente un conector de interfaz de usuario acoplado operablemente al motor de ejecución y dispuesto para proporcionar parámetros de política de gestión de contenido desde por lo menos uno de: por lo menos un dispositivo móvil que es servido por la red inalámbrica, la red inalámbrica en sí misma, o un usuario de por lo menos un dispositivo móvil que es servido por la red inalámbrica.

En algunos ejemplos, el aparato de gestión de datos de contenido móvil antimalware puede derivar los parámetros de política de gestión de contenido a partir de la información basada en ubicación proporcionada desde un sensor de ubicación dentro de por lo menos un dispositivo móvil o dentro de una entidad de red inalámbrica que sirve a por lo menos un dispositivo móvil, por ejemplo, GPS, GLOSNASS o dispositivo de triangulación de red inalámbrica, o similares. La información basada en ubicación se puede utilizar para habilitar un método o enlace de comunicaciones diferente y alternativo entre por lo menos un dispositivo móvil y otro dispositivo de envío o recepción. Este enlace de comunicaciones alternativo se puede utilizar para redireccionar los datos de contenido si se considera un enlace inalámbrico original, por ejemplo, cualquiera de los siguientes: demasiado ancho de banda restringido, demasiado costoso y/o demasiado inseguro.

En algunos ejemplos, por lo menos un generador de credenciales puede comprender múltiples generadores de credenciales, cada uno de los múltiples generador de credenciales en diferentes ubicaciones dentro del motor de gestión de contenido, y cada uno dispuesto para volver a generar de credenciales los datos de contenido antes de una etapa de procesamiento posterior. La etapa de procesamiento posterior puede incluir cualquiera de una etapa de regeneración, etapa de filtrado, etapa de gestión de contenido o etapa de validación de contenido.

En algunos ejemplos, el aparato de gestión de datos de contenido móvil puede estar ubicado en cualquier lugar fuera (y adecuadamente conectado a la red inalámbrica) y/o dentro de la red inalámbrica, en la que el aparato puede llevar a cabo una o más de las funciones descritas. El aparato descrito, o instancias del mismo, se puede colocar o ubicar, física y/o lógicamente, en un borde de la red inalámbrica para que actúe como una interfaz con otra red de comunicaciones a la que se conecta la red inalámbrica objeto para la comunicación entre ellos, para, por lo tanto, pasar los archivos electrónicos de gestión por contenido a través de la red inalámbrica, o pasar entre la red inalámbrica y la otra red de comunicaciones.

En algunos ejemplos, se puede proporcionar el aparato de gestión de datos de contenido móvil como un aparato de gestión de datos de contenido móvil distribuido que tiene submódulos dispuestos para llevar a cabo etapas de procesamiento en diferentes ubicaciones dentro de la red inalámbrica. Los submódulos distribuidos se pueden ubicar junto con algunos de los otros submódulos y/o con otras entidades que proporcionan la red inalámbrica u otra red de comunicaciones a la cual se conecta la red inalámbrica para la comunicación entre ellos. Los submódulos también se pueden ubicar dentro de uno o más de los dispositivos móviles servidos por la red inalámbrica, o a través de la red inalámbrica y uno o más de los dispositivos móviles.

En algunos ejemplos, el aparato de gestión de datos de contenido móvil es un aparato de gestión de datos de contenido móvil de única instancia, y la única instancia comprende adicionalmente por lo menos un segundo filtro para filtrar la representación genérica etiquetada de los datos de contenido para eliminar datos de contenido no referenciados o inalcanzables después de que el motor de gestión de contenido ha aplicado una política de gestión de contenido predeterminada to una representación genérica etiquetada filtrada de los datos de contenido.

También se proporciona un dispositivo móvil que comprende una aplicación de lado del dispositivo móvil configurada para uso con el aparato de gestión de datos de contenido móvil antimalware descrito en este documento, en el que aplicación de lado del dispositivo móvil puede comprender por lo menos una función de lector genérico para permitir el uso y/o manipulación de los datos de contenido incluidos dentro de cualquier instancia de representación genérica etiquetada de los datos de contenido, y posiblemente una porción de la consola de gestión operable para permitir un usuario del dispositivo móvil para configurar o modificar la política de gestión de contenido que se va a aplicar al mismo dispositivo móvil, o otros dispositivos móviles servidos por la red inalámbrica.

El(los) dispositivo(s) móviles proporcionados de acuerdo con los ejemplos de la invención también pueden proporcionar una o más de las etapas del proceso de gestión de contenido general, más particularmente la etapa de regeneración (principalmente para la salida archivos al usuario del dispositivo móvil), y posiblemente una etapa de generación de credenciales (para la entrada de datos de contenido del usuario del dispositivo móvil, para enviar a través de la red inalámbrica) En estos ejemplos, el dispositivo móvil proporciona una funcionalidad de gestión de contenido de entrada y salida de extremo a extremo completa.

Los ejemplos también proporcionan un método de gestión de datos de contenido móvil antimalware, para uso en gestionar por contenido un archivo electrónico de entrada que contiene datos de contenido para ser enviados a través de una red inalámbrica que comprende por lo menos un dispositivo móvil que es servido por la red inalámbrica, el método comprende generar de credenciales los datos de contenido incluidos dentro del archivo electrónico de entrada en una representación genérica etiquetada de los datos de contenido, gestionar por contenido la representación genérica etiquetada de los datos de contenido para aplicar una política de gestión de contenido predeterminada a la representación genérica etiquetada de los datos de contenido para formar datos de contenido gestionados por contenido, validar los datos de contenido gestionados por contenido representados en la representación genérica etiquetada para asegurar dichos datos de contenido gestionados por contenido se ajuste a cualesquier limites predefinidos y reglas aplicadas a cada forma de datos de contenido que aparece en los datos de contenido del archivo electrónico de entrada, para formar datos de contenido gestionados por contenido validados, y emitir un archivo electrónico de salida sustituto derivado de los datos de contenido gestionados por contenido validados.

En algunos ejemplos, el método puede comprender adicionalmente filtrar la representación genérica etiquetada de los datos de contenido para eliminar datos de contenido no referenciados o inalcanzables.

En algunos ejemplos, el método puede comprender adicionalmente regenerar los datos de contenido en un archivo electrónico de salida sustituto derivado de los datos de contenido gestionados por contenido validados al regenerar una nueva instancia de un archivo electrónico en una especificación de tipo de archivo predeterminada para su uso posterior por la red inalámbrica en lugar de del archivo electrónico o al emitir los datos de contenido gestionados por contenido validados como una representación genérica etiquetada.

En algunos ejemplos, el método puede comprender adicionalmente normalizar el archivo electrónico de salida sustituto a una versión predeterminada de la especificación de tipo de archivo predeterminada.

En los ejemplos, el método comprende adicionalmente proporcionar parámetros de política de gestión de contenido indicativos de, o para uso en aplicar, la política de gestión de contenidos que estará vigente a través de un motor de ejecución acoplado operablemente al motor de gestión de contenido.

En los ejemplos, el método comprende adicionalmente proporcionar parámetros de red al motor de ejecución a través de un monitor de parámetros de red acoplado operablemente al motor de ejecución, con el fin de proporcionar medios para configurar o modificar los parámetros de política de gestión de contenido.

En algunos ejemplos, el método puede comprender adicionalmente proporcionar parámetros de política de gestión de contenido, a través de un conector de interfaz de usuario acoplado operablemente al motor de ejecución, desde por lo menos uno de: por lo menos un dispositivo móvil que es servido por la red inalámbrica, la red inalámbrica en sí misma, o un usuario de por lo menos un dispositivo móvil que es servido por la red inalámbrica.

En algunos ejemplos, el método puede comprender adicionalmente proporcionar múltiples generadores de credenciales en diferentes ubicaciones dentro del motor de gestión de contenido, cada uno se dispone para volver a generar de credenciales los datos de contenido antes de una etapa de procesamiento posterior.

En algunos ejemplos, el método puede comprender adicionalmente ubicar el aparato de gestión de datos de contenido móvil dentro de la red inalámbrica, o en un borde de la red inalámbrica para actuar como una interfaz con otra red de comunicaciones, para, por lo tanto, pasar los archivos electrónicos de gestión por contenido a través de la red inalámbrica o entre la red inalámbrica y la otra red de comunicaciones.

En algunos ejemplos, el método puede comprender adicionalmente distribuir submódulos del aparato de gestión de datos de contenido móvil a través de diferentes ubicaciones dentro de la red inalámbrica, cada submódulo se dispone para llevar a cabo una etapa de procesamiento diferente de un proceso de gestión de contenido general.

En algunos ejemplos, el método puede comprender adicionalmente una segunda etapa de filtro para filtrar la representación genérica etiquetada de los datos de contenido para eliminar datos de contenido no referenciados o inalcanzables después de que el motor de gestión de contenido ha aplicado una política de gestión de contenido predeterminada a una representación genérica etiquetada filtrada de los datos de contenido.

Estos y otros aspectos de la invención serán evidentes y se aclararán con referencia a las realizaciones descritas a continuación.

Las realizaciones de ejemplo se pueden denominar como “antimalware” o como que proporciona “protección contra malware”, y esta terminología puede incluir cualquier protección adecuada contra malware, en el que dicho malware puede incluir, por ejemplo, virus, troyanos y otras formas de contenido malicioso Sin embargo, el aspecto antimalware se proporciona particularmente en los ejemplos de la invención mediante solo la regeneración de datos de contenido bien conocidos en archivos electrónicos de salida o intermedios, definidos por ciertos criterios de datos de contenido bien conocidos. Durante la operación, los ejemplos de (el) los aparato(s) y método(s) divulgado(s) pueden operar en uno o más archivos electrónicos que son recibidos o enviados por entidades dentro de una red inalámbrica, o comunicados de otra manera a través de la red inalámbrica, que incluye cualquier porción cableada de dichas redes inalámbricas. Múltiples redes inalámbricas pueden estar involucradas, o cubiertas por ejemplos de la invención.

Los ejemplos pueden evaluar cada byte en un archivo electrónico original y solo regenerar una o más instancias completamente nuevas de ese archivo electrónico original en la misma especificación/formato de tipo de archivo como el archivo electrónico original, y uno que cumpla con ciertos criterios de bien conocido, en un proceso o procesos de reescritura posterior. Como resultado, el(los) aparato(s) y método(s) divulgado(s) son capaces no solo de proporcionar protección contra virus, sino también proporcionar gestión de datos de contenido y ahorrar en el ancho de banda de la red al permitir que solo los datos de contenido basados en archivos apropiados (por ejemplo, considerados permitidos) para ser regenerados durante el proceso de reescritura. Una extensión adicional de la operación puede ser permitir que un usuario o administrador de red determine el tipo apropiado (por ejemplo, considerado permitido) de los datos de contenido basados en archivos que desean permitir que se transmitan a través de la red inalámbrica, y/o en/fuera de la(s) máquina(s) del usuario, que se pueden denominar un punto terminal o dispositivo móvil (y se debe entender que incluye, entre otros, dispositivos como teléfonos móviles, ordenadores de escritorio, ordenadores portátiles, ordenadores tipo tableta, teléfonos, ‘phablets’, y cualquier otro dispositivo informático que se pueda conectar a través de una red de comunicaciones inalámbricas).

En algunos ejemplos, los administradores y/o usuarios pueden ser capaces de controlar los datos de contenido permitidos a través de una consola de gestión. La consola de gestión puede ser capaz de determinar qué datos de contenido basados en archivos están permitidos y qué contenido no (es decir, contenido no permitido). La consola de gestión se puede ubicar dentro de la red inalámbrica central, o en uno o más de los dispositivos móviles que son servidos por la red inalámbrica, por ejemplo, dentro de una aplicación del lado del dispositivo móvil. El(los) aparato(s) y método(s) divulgado(s) también pueden permitir al administrador/usuario determinar qué acción se debe tomar con cualquier información de contenido no permitida. Dichas acciones podrían incluir si se elimina una parte o la totalidad de los datos de contenido no permitidos durante una etapa de reescritura del método general, o nunca se incluyen los datos de contenido no permitidos en cualquier etapa de regeneración posterior. El método también puede permitir que un archivo electrónico continúe a su destino previsto o que ponga en cuarentena el archivo electrónico y detenga el viaje del archivo cualquier adicional, o permitir que solo un archivo electrónico funcionalmente reducido continúe su viaje.

En realizaciones de ejemplo, un nodo o porción de procesamiento solo ‘sintáctico’ del método se puede llevar a cabo en un punto en una red inalámbrica, y este punto en la red inalámbrica puede incluir la totalidad o parte de una subfuncionalidad discreta (por ejemplo, el generador de credenciales, filtros previos/posteriores, gestión de datos de contenido y validador) descritos a continuación. El procesamiento solo sintáctico puede ocurrir, por ejemplo, donde se requiere un rendimiento más rápido de la red inalámbrica general, o una parte de la misma (que incluye las porciones cableadas). El uso de dicho procesamiento solo ‘sintáctico’ puede detectar archivos, tipos de archivos y/o datos de contenido basados en archivos dentro de un archivo electrónico que no es permitido, es decir, “archivos ofensivos” (bajo una política predefinida, o de otra manera, como se describe más detalladamente a continuación) más rápidamente. Por lo tanto, los archivos sintácticos ofensivos (en su totalidad, o solo en parte) se pueden eliminar de la red inalámbrica general. Alternativamente, o adicionalmente, los archivos ofensivos se pueden pasar a un nodo adicional, o subrutina de método, para análisis adicional. El único nodo o porción de procesamiento

‘sintáctico’ puede ser una etapa inicial, antes de que se instiguen los otros nodos o porciones de procesamiento, para eliminar el archivo o los datos de contenido ofensivos lo antes posible.

Los nodos o porciones de procesamiento solo ‘sintáctico’ pueden utilizar un procesador de ‘reglas básicas’ para detectar y eliminar archivos, o datos de contenido basados en archivos del mismo, que claramente no están correctamente formados sintácticamente (es decir, el procesamiento sintáctico se ocupa de garantizar que los elementos del archivo y/o la estructura de datos de contenido basado en archivos sean correctos). Esta es una etapa particularmente beneficiosa del procesamiento de archivos de acuerdo con los ejemplos de la invención, porque el análisis estadístico de datos de red de la vida real ha mostrado que más del 90% de todos los ataques basados en malware pueden ser de este tipo “sintáctico-ofensivo”, es decir, basado en datos de contenido de archivo sintácticamente incorrectos. Más aún, la eliminación de archivos que fallan en una revisión sintáctica puede mantener un flujo de datos muy alto a través de la red inalámbrica (o por lo menos una velocidad de datos más alta de lo que sería el caso), ya que los datos de contenido no permitidos se pueden eliminar y/o ignorar previamente, y por lo tanto, evitan el desperdicio de recursos de redes subsiguientes (que incluyen ancho de banda y costes de procesamiento, entre otras cosas). Por ejemplo, cualquier descompresión posterior.

Los ejemplos pueden proporcionar una pluralidad de (sub)etapas de procesamiento, en las que cada (sub)etapa se puede configurar para llevar a cabo una verificación diferente. Más aún, al realizar verificaciones básicas primero, los ejemplos de la invención pueden distribuir la carga de procesamiento a través de múltiples entidades dentro de la red inalámbrica, por ejemplo, las verificaciones básicas (rápidas) se pueden realizar en uno(s) (o múltiples, previos) nodo(s), con cualquier verificación más profunda adicional, realizada en otro lugar, posteriormente (por ejemplo, más cerca del usuario). Efectivamente, esto permite que los archivos maliciosos o no deseados, o porciones de los mismos, es decir, los datos de contenido no permitidos, se detengan previamente en la red inalámbrica y, por lo tanto, no ocupen ancho de banda ni ciclos de procesamiento en una etapa posterior.

El PDF (Formato de documento portátil, generalmente abreviado como.pdf como la extensión del archivo que indica su tipo) es sólo un ejemplo de tipo de archivo de muchos (por ejemplo, Word.doc(x), Excel.xls(x), PowerPoint.ppt(x),.rtf,.html,.tif,.jpg,.gif, etc.) de la clase de tipo de archivo al que ejemplos de del tipo de archivo al que se pueden aplicar los ejemplos de la invención. En el ejemplo de PDF, el archivo electrónico se construye a partir de nodos que están conectados por una estructura de árbol. Es bastante frecuente que estas ramas se rompan cuando los archivos son guardados por ciertas aplicaciones ‘lectoras’ mal implementadas. Por ejemplo, en lugar de reescribir correctamente todo el archivo, estas aplicaciones ‘lectoras’ mal implementadas rompen los enlaces dentro del archivo electrónico respectivo, que son necesarios para el análisis aprobado utilizado para dicho tipo de archivo electrónico, lo que hace que los datos de contenido sean inaccesibles y están ‘ocultos’. Más aún, esto significa que el tamaño del archivo electrónico aumenta a pesar de que los datos de contenido que causan el aumento del tamaño no son deseados. En los ejemplos de la invención, se puede utilizar una etapa de prefiltro para eliminar estos datos de contenido superfluo, no referenciables/inalcanzables, y por lo tanto ahorrar el ancho de banda necesario para transmitir un archivo electrónico a través de la red de comunicaciones inalámbricas y similares. A continuación, el término ‘formato de archivo’ puede ser sinónimo de “tipo de archivo”, según el uso. De manera similar, ‘red inalámbrica’ y ‘red de comunicaciones inalámbrica’ se pueden utilizar indistintamente, a menos que se indique lo contrario.

Breve descripción de los dibujos

Se describirán detalles, aspectos y realizaciones adicionales de la invención, solo a modo de ejemplo, con referencia a los dibujos. En los dibujos, los números de referencia similares se utilizan para identificar elementos similares o funcionalmente similares. Los elementos en las Figuras se ilustran por simplicidad y claridad y no necesariamente han sido dibujados a escala.

La Figura 1 muestra un esquema de una red móvil de ejemplo con una pluralidad de dispositivos móviles;

La Figura 2 muestra un esquema de una red móvil de ejemplo con una pluralidad de dispositivos móviles de acuerdo con una primera realización de ejemplo de la presente invención;

La Figura 3 muestra un esquema de una red móvil de ejemplo con una pluralidad de dispositivos móviles de acuerdo con una segunda realización de ejemplo de la presente invención;

La Figura 4 muestra un ejemplo de un dispositivo de red de única instancia de acuerdo con una primera realización de ejemplo de la presente invención;

La Figura 5 muestra una conversión (singular) de ejemplo de un archivo electrónico de entrada original a un archivo electrónico de salida modificado singular (es decir, gestionado por contenido), de acuerdo con un ejemplo de la invención;

La Figura 6 muestra una conversión (distribuida) de ejemplo de un archivo electrónico de entrada original a un archivo electrónico de salida modificado singular (es decir, gestionado por contenido), de acuerdo con un ejemplo de la invención;

La Figura 7 muestra procesos de gestión de datos de contenido de ejemplo de un método de acuerdo con un ejemplo de la invención;

La Figura 8 muestra una porción de generación de credenciales y regeneración de ejemplo de un método de acuerdo con un ejemplo de la invención.

Descripción detallada de las realizaciones preferidas.

Debido a que las realizaciones ilustradas de la presente invención pueden implementarse en su mayor parte utilizando componentes y circuitos electrónicos conocidos por aquellos expertos en la técnica, los detalles no se explicarán en mayor medida de lo que se considera necesario como se ilustró anteriormente, para su comprensión y apreciación de los conceptos subyacentes de la presente invención y con el fin de no ofuscar o distraer las enseñanzas de la presente invención.

Los ejemplos de la presente invención pueden proporcionar la transcodificación de un tipo de datos de contenido a otro, llevada a cabo con base en una política de gestión predefinida. Esta política de gestión predefinida puede ser controlada por un usuario o el administrador (del sistema) a través de, por ejemplo, una consola de administración, o tal vez un representante de seguridad autorizado de la organización haciendo uso de una o más redes inalámbricas de acuerdo con los ejemplos de la invención. El control puede tomar la forma de una aplicación sobre un dispositivo móvil, lo que permite al usuario respectivo o al administrador (del sistema) controlar el nivel de datos de contenido considerados permitidos. Por lo tanto, el control de un nivel de datos de contenido considerados permitidos puede, por ejemplo, controlar un nivel de compresión en uso en la red inalámbrica, o porción de la misma, en un momento dado. El control también puede tomar la forma de control directo sobre el ancho de banda real o asumido, los tipos de archivos permitidos/no permitidos específicos, los tipos de contenido de datos y similares, y estos pueden ser aplicados por un motor de ejecución.

Adicionalmente, en algunos ejemplos, un mecanismo de control automatizado puede proporcionarse adicional o alternativamente. El mecanismo de control automatizado puede ser controlado por la red inalámbrica en la que se pueden implementar/situar ejemplos de la invención. El mecanismo de control automatizado puede ajustar dinámicamente la(s) política(s) de gestión de datos de contenido dependiendo de diferentes factores, por ejemplo, los factores ambientales o comerciales que pueden afectar un canal de datos entre un dispositivo móvil y la red inalámbrica en la que opera el dispositivo móvil. Entonces, por ejemplo, un factor ambiental puede ser que el canal de datos está experimentando un ancho de banda bajo debido a la interferencia. En este tipo de situación, los datos de contenido considerados permitidos y, por lo tanto, los datos de contenido de un archivo electrónico se pueden ajustar automáticamente, por ejemplo, mediante una política de gestión de datos de contenido más agresiva, para reducir los requisitos de ancho de banda de datos para enviar o recibir un archivo electrónico a través de la red inalámbrica (por ejemplo, las imágenes se pueden eliminar de los documentos, dejando solo texto). También se pueden utilizar otros factores ambientales para controlar los datos de contenido recibidos y enviados a un dispositivo móvil a través de un enlace de comunicaciones inalámbricas, en la forma de un archivo electrónico. Los datos de contenido también pueden estar incluidos en construcciones alternativas distintas de “archivos”, y el término “archivo” o “archivos” a lo largo de esta descripción se pueden interpretar como que incluye cualquier contenedor de datos alternativo.

Otro ejemplo de factor más comercial puede ser que el dispositivo móvil esté en itinerancia sobre una red inalámbrica diferente, de tal manera que los cargos por datos son más altos que en la red inalámbrica doméstica. En tal caso, el ancho de banda de los datos puede ser nuevamente limitado, a fin de reducir los cargos por datos de itinerancia. La detección de un estado de itinerancia se puede llevar a cabo de manera lógica, utilizando los datos de conectividad disponibles en la red inalámbrica o dispositivo móvil, o se puede llevar a cabo utilizando información de posicionamiento, es decir, información basada en ubicación medida directamente, por ejemplo, a partir de lecturas de GPS derivadas de un sensor/receptor de GPS, u otro tipo de sensor de ubicación dentro de uno o más dispositivos móviles. Por lo tanto, la información basada en ubicación puede ser particularmente útil para determinar el coste de los datos, que luego puede retroalimentar para determinar un nivel adecuado de política de gestión de datos de contenido en uso. La determinación de un nivel adecuado de gestión de datos de contenido puede ser estática o dinámica.

La información basada en ubicación se puede derivar de sensores de posicionamiento, tales como sensores de posicionamiento satelital GPS, GLOSNASS y/o Galileo, o se pueden derivar por otros medios adecuados, tales como sensores de inercia o medios de triangulación inalámbricos (por ejemplo, utilizando múltiples señales de red inalámbrica terrestre con técnicas de triangulación para proporcionar de esta manera una posición triangulada). La información basada en ubicación también puede ser deducida por el dispositivo de red/dispositivo móvil, ya que el dispositivo de red/dispositivo móvil puede conocer la forma de enrutamiento a la estación base apropiada con la que

se está comunicando el dispositivo móvil (por ejemplo, un teléfono inalámbrico), es decir, una evaluación de la ubicación más lógica.

En algunos ejemplos, la información basada en ubicación puede indicar que el dispositivo móvil se encuentra en un área en la que el uso de la red inalámbrica normal por parte del dispositivo móvil (ya sea para algunos o todos los datos de contenido) se considera indeseable o no es permitida por la política de gestión de contenido vigente. Esto puede suceder, por ejemplo, debido a que solo el ancho de banda restringido está disponible para el dispositivo móvil a través de la red inalámbrica (o porción de la misma) que sirve al dispositivo móvil en ese momento, o la red inalámbrica se considera insegura para el paso de los datos de contenido que se van enviar/recibir (por ejemplo, porque el dispositivo móvil está en itinerancia en otra red inalámbrica en ese momento). El ancho de banda bajo/restringido solo puede estar disponible para el dispositivo móvil si, por ejemplo, el dispositivo móvil respectivo se encuentra en un borde del área de recepción de la red inalámbrica, lo que puede significar que solo se proporciona con conectividad de tipo 2G, mientras que el núcleo de la red inalámbrica tiene una conectividad de tipo 3G. Sin embargo, el ancho de banda restringido también se puede deber a otros factores, que incluyen el hecho de que el dispositivo móvil actualmente está en itinerancia en otra red inalámbrica, por lo que el ancho de banda restringido se debe a consideraciones monetarias o de seguridad, en lugar de problemas reales de provisión de servicios, per se.

Independientemente de por qué el ancho de banda se considera demasiado restringido/restrictivo o de otra forma inseguro o inadecuado para el uso del dispositivo móvil respectivo (según la política de gestión de contenido vigente), el dispositivo móvil respectivo, o la aplicación/módulo de gestión de contenido del mismo, puede reenrutar las comunicaciones desde/hacia el dispositivo móvil respectivo a través de un canal de comunicaciones alternativo en su lugar. Esto puede ser particularmente beneficioso cuando el dispositivo móvil respectivo puede estar provisto, por ejemplo, de un sistema de transceptor de comunicaciones por satélite de mayor velocidad (pero con una latencia más baja) así como del sistema de transceptor de comunicaciones inalámbricas terrestres. Por ejemplo, para utilizar con el sistema de satélites Iridium, GlobalStar, INMARSAT o cualquier otro sistema de comunicaciones satelital global de órbita terrestre alto/medio/bajo, o cualquier sistema de satélites que pueda proporcionar cobertura global con una alta capacidad de velocidad de datos. En estos ejemplos, el sistema de comunicaciones satelitales puede proporcionar comunicaciones inalámbricas de alta velocidad desde el dispositivo móvil respectivo hasta l satélite (por ejemplo, 10's de Mbit a 100's de Mbit, o incluso enlaces multi-Gbit), operables mientras el satélite está dentro de una línea de visión (por ejemplo, encima del horizonte/ecos del suelo) de la ubicación actual del dispositivo móvil. El satélite puede tener medios de almacenamiento de datos locales significativos (es decir, en el satélite) para conservar esta información hasta tal momento que el satélite haya orbitado a otra ubicación segura, por ejemplo, inicio (generalmente de vuelta en la red inalámbrica principal/"normal", para transmisión posterior del mismo). Luego, el satélite puede enviar los datos del contenido almacenado a una estación receptora en la red inalámbrica doméstica. Esto se puede denominar como una capacidad de "almacenamiento y envío". Esto sería particularmente útil cuando el conjunto de datos de contenido que se enviará sea cualquiera de los siguientes: muy grande (por ejemplo, multi-gigabytes, o más), lo que puede suceder cuando se hace recopilación de datos significativa en una ubicación remota (por ejemplo, estudios sismológicos) o muy sensible (por ejemplo, un plan de negocios comercial realizado en el sitio en la ubicación del sitio del cliente en el extranjero). Al utilizar dichos enlaces de comunicaciones alternativos, los datos de contenido se pueden mantener con un tamaño de conjunto de datos más alto o una mayor seguridad de transmisión (es decir, sin indagación, etc.) de lo que podría ser el caso.

Las políticas de gestión de datos de contenido, controladas y/o configuradas por, por ejemplo, parámetros de política de gestión de contenido adecuados utilizados dentro del sistema, también se pueden determinar con base en las capacidades reales del dispositivo móvil/punto terminal, en el que, por ejemplo, las capacidades del dispositivo móvil/punto terminal se pueden determinar por el tamaño de pantalla del punto terminal en cuestión, y/o los recursos de procesamiento disponibles (por ejemplo, velocidad, número, profundidad de bits de la CPU, caché asociado y/o tamaño de RAM, velocidad de RAM, disponibilidad de coprocesadores o núcleos en un dispositivo de múltiples núcleos, etc.). El nivel de recursos de procesamiento disponibles en cualquier dispositivo móvil/punto terminal dado que se puede conectar y hacer uso de los ejemplos de la invención puede determinar un nivel dado de capacidad del dispositivo móvil respectivo. Por ejemplo, determinar si un dispositivo móvil/punto terminal se considera un "dispositivo de baja capacidad", "dispositivo de capacidad media"; y/o "dispositivo de alta capacidad". Los niveles de capacidad utilizados también pueden ser (re)ajustados con el tiempo, a medida que las capacidades se mueven, y las tecnologías de dispositivos móviles más nuevas sustituyen a las tecnologías existentes.

Los dispositivos móviles se pueden someter a partición adecuadamente en grupos de dispositivos móviles similares o similares de acuerdo con sus capacidades. Por ejemplo, los aparatos, métodos y sistemas propuestos se pueden disponer para colocar cualquier dispositivo móvil/punto terminal que se conecte a la red de comunicaciones inalámbrica en la que se ejemplifican las realizaciones de la invención, en tres categorías amplias de dispositivo: "Dispositivo de baja capacidad", por ejemplo típico de los teléfonos pequeños que pueden abrir documentos de imagen, así como tener una capacidad de navegación limitada; "dispositivo de capacidad media", por ejemplo los teléfonos inteligentes, y los dispositivos típicos que pueden abrir documentos tales como Microsoft Word, Excel, PDF, aunque con capacidad limitada, pero tienen una experiencia de navegación web mucho más rica; "Dispositivo de alta capacidad", por ejemplo ordenadores tipo Tableta, PC, ordenador portátil, es decir, la caracterización típica

de dispositivos que pueden ofrecer una capacidad de análisis de documentos completa, así como una completa experiencia de navegación web, y similares.

Teniendo en mente estas categorizaciones de capacidad de dispositivo móvil, los ejemplos de la invención pueden tener una política de regeneración de archivos (es decir, una política para la reescritura de nuevas instancias del mismo tipo que el archivo electrónico de entrada original) configurada para reflejar la capacidad del dispositivo móvil/punto terminal que está destinado a recibir los datos de contenido/archivo electrónico en cuestión. En algunos ejemplos, puede haber múltiples tipos de archivos de salida regenerados a partir de un único archivo electrónico de entrada, de tal manera que se puede proporcionar cada una de las muchas categorías de dispositivos, al mismo tiempo que se minimizan los recursos de red inalámbrica necesarios para suministrar cada versión a los dispositivos móviles respectivos. Esto se puede extender, de tal manera que, por ejemplo, los datos de contenido se pueden actualizar automáticamente a medida que el dispositivo móvil cambia para un usuario determinado. Por ejemplo, un usuario puede actualizar un dispositivo móvil y automáticamente tener la versión actualizada del archivo electrónico que se proporciona en la próxima revisión de ese archivo, en una fecha posterior. O el mismo dispositivo móvil puede recibir un archivo electrónico gestionado con datos de contenido originales mientras que está en itinerancia en la red inalámbrica de otro país, pero al regresar al Reino Unido, el archivo original (más) completo se proporciona automáticamente en la próxima revisión. Otros ejemplos incluyen: si un pequeño teléfono, es decir, un “dispositivo de baja capacidad” está destinado a recibir un archivo electrónico a través del sistema de gestión de datos de contenido antimalware descrito, entonces hay poco sentido en los aparatos, métodos o sistemas descritos que regeneran datos de contenido que el dispositivo móvil/punto terminal de “baja” capacidad” no puede mostrar, y los ejemplos de la invención se pueden disponer de manera adecuada para no regenerar los datos de contenido que el dispositivo móvil de destino no puede mostrar o utilizar, preservando de esta manera los datos no utilizables de transferencia de desperdicio de ancho de banda de red (hasta ahora). Es decir, el nivel de regeneración de datos de contenido se puede determinar con base, entre otras cosas, en la categorización de capacidades determinada o predefinida y que pueden variar, y la varianza a la que reacciona la red inalámbrica global, de forma dinámica (es decir, sobre la “marcha”).

Los ejemplos de la invención también pueden ayudar a mantener la segregación de dominios cruzados al utilizar la transformación de archivos. Esto se debe a que los dispositivos móviles/puntos terminales y la infraestructura de red inalámbrica de acuerdo con realizaciones de ejemplo de la invención pueden segregar los datos de negocios de los usuarios a partir de sus datos personales al anular efectivamente los dos dominios. Por ejemplo, cuando un documento necesita viajar desde un dominio de ‘alta confianza’ hasta un dominio de ‘baja confianza’, una realización de la invención puede proporcionar esta verdadera capacidad de dominio cruzado al realizar la función de transformación en los datos, ya sea que se encuentra en el punto terminal o se distribuye a través de dicha red inalámbrica. Es decir, los datos de contenido de formato de archivo se transforman a partir de su forma original a una forma intermedia, generalizada, y luego se regeneran a una forma final. Por lo tanto, nada que sea desconocido o no contabilizado puede pasar a través de esta barrera de aislamiento, ya que, efectivamente, se ha eliminado de un dominio (o formato de tipo de archivo) en el que son posibles los ataques, a un dominio inerte (o forma libre del tipo de archivo) en el que no se puede lanzar un ataque.

Como se mencionó anteriormente, las formas de realización de ejemplo de la invención pueden transformar los datos de contenido de una forma original en una forma intermedia, generalizada o una representación interna de los datos de contenido. Esta transformación puede incluir aplicar la gestión de datos de contenido selectiva de los datos de contenido, y luego regenerar un nuevo archivo sustituto (es decir, una nueva instancia de archivo, construida desde cero y que consiste solo en datos de contenido que son bien conocidos del archivo electrónico original). El archivo sustituto regenerado puede estar en una forma genérica. Esta forma genérica se puede considerar una barrera de seguridad efectiva de “espacio de aire”, y puede proporcionar un aislamiento total del archivo electrónico de entrada no confiable al archivo electrónico de salida saneado y regenerado (ya sea salida en forma genérica en sí misma o procesada posteriormente como una nueva instancia de un archivo en el mismo tipo de archivo que el archivo de entrada original). Como se discute adicionalmente, los aparatos y métodos de gestión de datos de contenido antimalware descritos se pueden realizar en una sola entidad dentro de la red inalámbrica, utilizando un proceso de paso único o de múltiples pasos, o en una serie de entidades distribuidas cada una realizando un paso individual diferente, como se describirá con más detalle a continuación. El espacio de aire se puede proporcionar mediante el uso de diferentes almacenamientos de memoria, separados lógica y quizás físicamente, y con un par de procesos de generación de credenciales y regeneración utilizados entre los almacenamientos de memoria, de tal manera que los datos de contenido se filtran efectivamente y/o se gestionan por contenido y, por lo tanto, solo los datos de contenido bien conocidos se pueden mover entre los dos almacenamientos de memoria, como se explicará con más detalle a continuación.

Los ejemplos de la presente invención también pueden proporcionar un aparato o método para gestionar datos de contenido en un dispositivo móvil, o en una red móvil/inalámbrica, que se puede aplicar a un archivo electrónico que contenga datos de contenido recibidos de una red externa y que se transfieran por la red inalámbrica. Red en la que se incorpora un ejemplo de la invención. El método puede comprender uno o más de: la transformación de un archivo electrónico recibido (o para ser enviado) en una representación genérica; aplicación de reparación a la representación genérica; aplicación de la gestión de datos de contenido a la representación genérica reparada para propósitos de reducción de ancho de banda y amenazas y/u otra política de restricción de datos de contenido;

validación de dicha representación genérica; y la regeneración de los datos de contenido como una nueva instancia de un archivo o representación genérica.

El método de gestión de datos de contenido móvil antimalware descrito en este documento proporciona la ventaja de permitir que los datos de contenido en una multitud de formatos de archivo se validen y estén sujetos a la política de gestión de datos de contenido utilizando un proceso definido de uno o múltiples pasos, el proceso se define en un formato común (es decir, utilizando una representación o representaciones genéricas), eliminando de esta manera el requisito de una multitud de rutinas de validación diferentes para cada formato de archivo que debe ser soportado por los aparatos y métodos de gestión de datos de contenido móvil antimalware. Cuando se trata de varios tipos de archivos, una mejora es tener una serie de generador de credenciales de archivos, que se describen más adelante, que convierten los datos desde un formato de archivo de entrada original a aquel de la representación genérica etiquetada al asignar una o más etiquetas para representar los datos de contenido, en los que los datos de contenido genéricos etiquetados se derivan de los datos de contenido originales. Este método reduce la complejidad del diseño, ya que permite, por ejemplo, una rutina de validación singular para todas las representaciones etiquetadas genéricas que se pueden utilizar sobre todos los diferentes formatos de archivo de entrada/salida (es decir, reutilizables en todos los formatos de archivo), en lugar de requerir la construcción de rutinas de validación individuales para cada uno de los formatos de archivo que se soportarán.

Adicionalmente, al transformar los datos de contenido entrantes desde un archivo electrónico hasta una representación genérica, también se elimina la necesidad de que un dispositivo móvil/punto terminal receptor tenga una serie de aplicaciones de software para analizar la multitud de formatos de archivos que se deben soportar para la visualización y/o manipulación sobre los dispositivos móviles. Efectivamente, los datos del contenido del archivo electrónico se representan en una forma que puede ser representada por una sola aplicación móvil, sin importar cuál sea el formato de archivo original.

Ahora sigue una explicación más detallada de los ejemplos de la invención, con referencia a las Figuras.

La Figura 1 muestra un esquema de un ejemplo de una red 100 de comunicaciones inalámbricas móvil con una pluralidad de dispositivos 120, 130, 140 móviles, conectados a la misma. En esta Figura se muestra una red 110 central (CN), que comprende, por ejemplo, una estructura 111 de conmutación de red central acoplada a uno o más controladores 112 de estación base (por simplicidad, se muestra un controlador de estación base singular). Un controlador 112 de estación base (BSC) puede estar acoplado operativamente a una o más estaciones 113 base, a través de uno o más enlaces 114 de comunicación. Puede haber varios controladores de estación base (no mostrados), cada uno de los cuales controla una serie de estaciones 113 base, como un subconjunto de la red 100 inalámbrico general. Una o más estaciones 113 base se pueden comunicar con la pluralidad de dispositivos 120-140 móviles utilizando cualquier estándar de comunicación inalámbrica, actualmente en uso, o aún no implementada, tal como, por ejemplo, pero no limitado a: GSM, GPRS, 3G, UTMS, W-CDMA, WiMAX, LTE, LTE-avanzado, etc. Dependiendo del estándar de comunicación en uso en la red inalámbrica que se describe a continuación (es decir, los elementos 100-103), los controladores de la estación base, la estructura 111 de conmutación CN y las estaciones base como se menciona a continuación se pueden llamar otras cosas (es decir, variantes), pero actúan de una manera funcionalmente similar. La funcionalidad también se puede dividir en las diferentes entidades de una manera diferente, pero actúan juntas de la misma manera, y por lo tanto, se debe interpretar que la siguiente información incluye todas dichas variantes.

Los enlaces 114 de comunicaciones utilizados para conectar las estaciones base 113 a los controladores de estación 112 base, pueden estar cableados (por ejemplo, Ethernet/enlaces IP ópticos) o enlaces inalámbricos (por ejemplo, enlace de microondas, etc.), o cualquier otro enlace de comunicaciones funcionalmente similar. Los enlaces 114 de comunicaciones pueden estar en cualquier topología adecuada (se muestra una topología en forma de estrella, pero también pueden estar en una formación de anillo o comprender múltiples enlaces entre diferentes estaciones 113 base, así como el controlador de estación 112 base). La red 110 central está normalmente conectada a Internet 105 en general, para interconectar los dispositivos 120-140 inalámbricos servidos por la red 100 inalámbrica, a Internet 105. La red 110 central puede comprender la estructura 111 de conmutación de red central, que se puede utilizar para enrutar datos, tales como voz, archivos electrónicos, mensajes de texto, etc., a un dispositivo móvil receptor adecuado en la red 100 inalámbrica en general. Dicho de otra manera, la estructura 111 de conmutación de red central se puede considerar la infraestructura principal que proporciona la capacidad de enrutamiento de llamadas y mensajes, que proporciona la interfaz entre la Internet 105 externa y el controlador 112 de estación base que realiza la administración y el control de las estaciones 113 base individuales que se conectan de forma inalámbrica a cada uno de dichos puntos terminales 120, 130 y 140 de dispositivos móviles, a través de enlaces 116 de comunicaciones inalámbricas.

Esta estructura 111 de conmutación de red central puede comprender una pluralidad de conmutadores de núcleo de red, enrutadores o similares (no mostrados individualmente) conectados entre sí por interconexiones bidireccionales adecuados, en los que, por ejemplo, cada conmutador o enrutador sirve una porción 100 de la red inalámbrica global, por ejemplo, un controlador 112 de estación base individual (BSC). Los conmutadores centrales se pueden conectar entre sí mediante enlaces 115 de comunicaciones troncales/ principales. Estos enlaces 115 de

comunicaciones troncales pueden ser un múltiplo de, u órdenes mayor capacidad de magnitud que los enlaces 114 individuales que conectan el BSC 112 a una estación 113 base, como se muestra.

La red 100 inalámbrica se puede conectar a, y por lo tanto servir, uno o más dispositivos/punto extremo 120-140 móviles. En la Figura 1, se muestran ejemplos de tres grandes grupos de dispositivos: un "dispositivo 120 de baja capacidad", por ejemplo, un teléfono generación anterior (también puede ser llamado un teléfono básico) que es capaz de enviar mensajes de texto, hacer llamadas y hacer uso de un conjunto muy limitado de medios, tales como imágenes en escala de grises y similares; un dispositivo 130 de "de capacidad media", por ejemplo, un teléfono con funciones (tal como, por ejemplo, un Blackberry) u otro dispositivo de teléfono inteligente, tal como, por ejemplo, un iPhone, etc., y capaz de abrir un mayor rango de archivos y datos de contenido de porción de archivo, etc. y/o un "dispositivo 140 de alta capacidad", tal como, por ejemplo, una ordenador tipo tableta, ordenador portátil u otro dispositivo con recursos sustanciales de procesamiento disponibles.

La Figura 2 muestra un esquema de un ejemplo de red 101 móvil/inalámbrica actualizada con una pluralidad de dispositivos móviles de acuerdo con una primera realización de ejemplo de la presente invención. La mayoría de la red 101 de comunicaciones móviles/inalámbricas es la misma que para la Figura 1, y en la que los elementos son los mismos, los números de referencia utilizados también son los mismos. Sin embargo, esta red 101 móvil/inalámbrica también incluye además una entidad 200 de gestión de contenido de acuerdo con una realización de ejemplo de la invención. Esta entidad 200 de gestión de contenido se puede ubicar en el borde de la red 110 central como se muestra, entre la red 110 central y la Internet 105 en general. Los dispositivos 120-140 móviles ahora también comprenden adicionalmente una aplicación 104 de dispositivo móvil, que proporciona la funcionalidad del lado del dispositivo móvil de los ejemplos de la invención. Un dispositivo móvil de la Figura 2 (es decir, cualquiera de 120, 130 y 140) puede ser un dispositivo que significa tener una pantalla, teclado de diferentes capacidades, un procesador y una memoria asociada para realizar tareas tales como recibir y realizar llamadas de voz, así como enviar y recibir mensajes de texto o correos electrónicos, o cualquier otro archivo electrónico. Adicionalmente, estos dispositivos móviles también pueden tener aplicaciones basadas en software que realizan una variedad de tareas que incluyen aplicaciones de software definidas por el usuario o "aplicaciones". En algunos ejemplos, una 'aplicación' 104 podría realizar la función de la entidad 200 de gestión de contenido (o el generador de credenciales 201, o cualquier otro submódulo de la entidad de gestión de contenido que se describe más adelante). Como el dispositivo 120, 130 o 140 móvil está ejecutando efectivamente la funcionalidad del lado del dispositivo móvil de los ejemplos de la invención, esto puede tomar la responsabilidad de realizar la funcionalidad descrita lejos de la red inalámbrica y la infraestructura asociada. Al ubicar la entidad 200 de gestión de contenido (o submódulo o parte del mismo, tal como generador de credenciales 201, etc.) como una aplicación 104 móvil o 'app' 104 en el dispositivo móvil, luego la gestión de datos de protección y de contenido de malware se puede realizar cuando el tráfico de datos se transmite desde el dispositivo móvil en lugar de ser recibido por el dispositivo móvil que ingresa a la red 110 central desde Internet 105. En la realización distribuida, detallada en la Figura 3, este elemento de 'app' 104 móvil sólo se necesita para llevar a cabo la funcionalidad descrita como el generador de credenciales 201, de tal manera que el teléfono móvil lleva a cabo la conversión al formato de etiquetado genérico en la preparación para un procesamiento adicional por otras entidades en la red inalámbrica como se describe.

La colocación de la entidad 200 de gestión de contenido en el borde de la red 101 inalámbrica, como se muestra, es un posicionamiento de ahorro de ancho de banda óptimo de dicha entidad 200 de gestión de contenido, ya que maximiza los ahorros de ancho de banda a través de la red 101 inalámbrica como un todo. Esto se debe a que la funcionalidad de gestión de contenido se realiza, en la entidad 200 de gestión de contenido, antes de que los datos del contenido del archivo ingresen a la red 101 inalámbrica desde Internet 105. Sin embargo, la entidad 200 de gestión de contenido también puede estar ubicada en otros lugares dentro de la red 101 inalámbrica para proporcionar otras optimizaciones en las que, por ejemplo, la resiliencia de datos y/o conectividad y el equilibrio de carga son tan importantes como la reducción de ancho de banda completo. La forma en que operan las entidades 200 de gestión de contenido de acuerdo con los ejemplos de la invención, se describirá con más detalle a continuación. Algunos ejemplos también pueden utilizar múltiples entidades 200 de gestión de contenido, por ejemplo, ubicadas en cada interfaz de red central/Internet y potencialmente en cada interfaz de red/dispositivo móvil. La última puede ser una interfaz compartida que da servicio a múltiples dispositivos móviles (por ejemplo, en una estación 113 base).

La Figura 3 muestra un esquema de una red 103 inalámbrica de ejemplo con una pluralidad de dispositivos 120-140 móviles de acuerdo con una segunda realización de ejemplo distribuida de la presente invención. Se apreciará que el nivel de distribución específico o topología utilizada en cualquier instancia de ejemplo de una red inalámbrica de acuerdo con la invención puede variar, y puede depender de los requisitos específicos de la instancia particular de una red inalámbrica en uso. Nuevamente, la mayoría de la red 103 móvil/inalámbrica es la misma que para la Figura 1, y en la que los elementos son los mismos, los números de referencia utilizados también son los mismos. Sin embargo, este ejemplo de red 103 móvil/inalámbrica difiere de la de la Figura 2, en que la entidad 200 de gestión de contenido se reemplaza por una versión distribuida, que comprende porciones distribuidas (es decir, subpartes, subprocesos o submódulos), por ejemplo, un generador de credenciales 201 de instancia de red central (mostrado como el "extremo frontal", es decir, punto de entrada de datos) de la entidad de gestión de contenido distribuido en la red 110 central) en este ejemplo ubicado en la posición "borde de la red" del original versión de instancia única de la entidad 200 de gestión de contenido, un prefiltro 211, un motor 213 de gestión de contenido, un postfiltro 215 (en

este ejemplo, estos tres submódulos se muestran como ubicados en conjunto con la estructura 111 de conmutación CN), un validador 217 de contenido (ubicado junto con el BSC 112) y una aplicación o módulo 204 de dispositivo móvil distribuido (que puede estar contenido dentro de cada uno de los dispositivos 120-140 móviles conectados a la red 103 de comunicaciones inalámbricas) que puede incluir una serie de submódulo/procesos en sí mismos, que incluyen el submódulo 219 de regenerador, y similares. La aplicación o módulo 204 de dispositivos móviles distribuidos puede ser igual o similar a la aplicación 104 de dispositivo móvil de instancia única (de la Figura 2), dependiendo de la extensión y/o la disposición específica de la distribución del proceso de gestión de contenido (por ejemplo, ubicación del generador de credenciales - en dispositivo móvil, o no). Es decir, la aplicación o módulo 204 de dispositivo móvil distribuida puede proporcionar algo del procesamiento distribuido de los datos de contenido, así como la funcionalidad de visualización. En esta Figura, se muestra un ejemplo más detallado de la aplicación o módulo 204 de dispositivo móvil, en este caso, con respecto al dispositivo 140 móvil de alto nivel, sin embargo, esto es solo un ejemplo, y la aplicación o módulo 204 de dispositivo móvil utilizado en dispositivos 120/130 de capacidad media o baja, también puede tomar la misma forma o similar (es decir, incluir uno o más de los submódulos descritos a continuación).

El ejemplo de aplicación o módulo 204 de dispositivo móvil más detallado comprende varios submódulos, que incluyen un regenerador 219, similar en función al regenerador descrito en otro lugar. También se muestra un submódulo 201' del generador de credenciales de la instancia del dispositivo móvil que funciona de manera similar a la del generador de credenciales que se describe en este documento. También puede haber un submódulo 271 de lectura adjunto que puede ser una función de lector de representación etiquetada genérica. La aplicación o módulo 204 de dispositivo móvil también puede comprender un submódulo 272 controlador que incluye, por ejemplo, un procesador para proporcionar los recursos de procesamiento del dispositivo móvil, en combinación con memoria y otro(s) submódulo(s) 273 de funcionalidad de procesamiento, que juntos pueden proporcionar funciones de submódulo 271 de lectura, el submódulo 201' de generador de credenciales y el submódulo 219 de regenerador. La(s) entrada(s) y la(s) salida(s) de/a la aplicación o módulo 204 de dispositivo móvil en su totalidad se pueden mostrar en la pantalla (no se muestra en la Figura para mayor claridad), bajo el control del usuario, a través del dispositivo de entrada del usuario (tampoco se muestra en la Figura para mayor claridad). El submódulo 272 controlador está acoplado comunicativamente a un submódulo 276 de enlace del sistema de comunicaciones inalámbrico principal/original (por ejemplo, un submódulo del sistema de transceptor 3G/4G) para proporcionar el enlace 116 de comunicaciones inalámbricas "normal" a la red 103 inalámbrica, a través de la estación 113 base. Sin embargo, la aplicación o módulo 204 de dispositivo móvil también puede proporcionar un sensor 274 de ubicación (por ejemplo, GPS, etc. que puede utilizar una antena 275 de satélite de solo recepción. La antena de solo recepción puede ser interna como se muestra, o externa al dispositivo móvil, acoplada al controlador 272, para proporcionar información basada en ubicación que también se puede utilizar para determinar los parámetros de la política de gestión de contenido (por ejemplo, control). Estos parámetros de la política de gestión de contenido derivado de la información basada en ubicación, en ciertas situaciones, tales como cuando determinan que la red 103 inalámbrica es insuficiente o demasiado lenta para las necesidades de los comunicadores actuales del dispositivo móvil, o simplemente demasiado inseguras, pueden invocar el uso de un submódulo del sistema de enlace de comunicaciones alternativo, por ejemplo, un sistema 277 de transceptor de satélite de alta velocidad independiente, que opera a través, por ejemplo una antena 278 de satélite bidireccional (normalmente externa, como se muestra, pero también puede ser interna), que puede proporcionar la velocidad y/o seguridad requerida de las comunicaciones al dispositivo móvil en la ubicación actual del dispositivo móvil, cuando sea necesario para los datos de contenido actuales que maneja el dispositivo móvil. Si los datos de contenido respectivos deben ser recibidos por el dispositivo móvil, se puede enviar una advertencia, por ejemplo, un indicador de notificación, o similar, al dispositivo móvil a través del enlace 116 inalámbrico normal, para permitir el encendido del submódulo 277 del sistema de comunicaciones alternativo listo para recibir cualquier información de contenido que requiera la utilización de esa ruta de comunicaciones alternativa.

La(s) operación(es) de, una interoperación entre, las porciones distribuidas del sistema de gestión de contenido general, especialmente de la red central, se describirán con más detalle a continuación. En los ejemplos, la entidad de gestión de contenido distribuido se puede distribuir a través de toda la red 110 central, la red "borde" inalámbrica (es decir, fuera del núcleo) (por ejemplo, estaciones base, su controlador (BSC) y otras entidades acopladas a BSC, y similares) e incluso los dispositivos móviles conectados al mismo. En cualquier caso, el (o por lo menos una primera instancia del) generador de credenciales puede permanecer en el borde de la red central (por ejemplo, la posición del generador de credenciales 201 en la Figura 3). El generador de credenciales 201 puede transformar el archivo electrónico en una representación genérica al mismo tiempo que realiza algunas comprobaciones sintácticas básicas de los datos de contenido, de tal manera que el ancho de banda se puede guardar en un punto de entrada en la red 110 central. Más aún, esta disposición también puede permitir que los datos de contenido ingresen a la red 110 central en una forma genérica, que no puede provocar ninguna actividad maliciosa ya que ya se ha transformado en una forma genérica inerte.

El generador de credenciales 201, prefiltro 211, motor 213 de gestión de contenido, postfiltro 215, validación 217 de contenido y aplicación 204 de dispositivo móvil distribuida (incluido el regenerador 219 y otros submódulos, cuando corresponda) se pueden proporcionar como complemento en los módulos de las entidades existentes dentro de la red 103 inalámbrica, por ejemplo, en forma de módulos adicionales para el BSC 112, la estructura 111 de conmutación de red central y los dispositivos 120-140 móviles (como se muestra), y/o pueden ser entidades

separadas adecuadamente interconectadas con dichas entidades de red inalámbrica existentes (en la que una "entidad de red inalámbrica" es cualquier elemento utilizado para proporcionar, o utilizado con, la red inalámbrica, es decir, entidades 111-140 de red inalámbrica, en los ejemplos mostrados en este documento).

La Figura 4 muestra un ejemplo de una entidad 200 de gestión de contenido de instancia única de acuerdo con una primera realización de ejemplo de la presente invención. La entidad 200 de gestión de contenido puede estar acoplada operativamente entre Internet 105 y la estructura 111 de conmutación de red central (como se muestra, sin embargo, también se pueden utilizar otras ubicaciones). La pluralidad de dispositivos 120-140 móviles también puede estar acoplada operativamente a la entidad 200 de gestión de contenido.

La entidad 200 de gestión de contenido puede comprender una serie de submódulos que interactúan, bajo control y/o configuración según los parámetros de la política de gestión de contenido, para llevar a cabo los métodos descritos a continuación (por ejemplo, como se describe en la Figura 7).

Los submódulos pueden comprender, por ejemplo, un conjunto de procesos 210 de gestión de contenido (y submódulos asociados) que se colocan en un flujo de trabajo principal a través del sistema de gestión de contenido entre Internet 105 y la estructura 111 de conmutación CN. El flujo de trabajo divulgado, o cualquiera de sus variantes, se puede ubicar entre otros elementos en red o redes diferentes. Los procesos 210 de gestión de contenido pueden comprender un módulo 201 de generador de credenciales, un módulo 211 de prefiltro, un módulo 213 de gestión de contenido, un módulo 215 de postfiltro, un módulo 217 de validación y un módulo 219 de regenerador. El prefiltro 211 y el postfiltro 215 son opcionales, por lo que se muestran en la línea de puntos en las Figuras. El módulo 201 de generador de credenciales se puede acoplar operativamente en la posición 212 inicial (es decir, el extremo frontal/punto de entrada de los datos de contenido en los procesos 210 de gestión de contenido), pero igual (cuando el generador de credenciales es "multitransmisión", es decir, capaz de que los generadores de credenciales 201 también se puedan ubicar en otras posiciones posteriores en el flujo de trabajo. Esto se muestra en la Figura como las líneas de puntos ubicadas después de cada submódulo subsiguiente, es decir, en las posiciones 214 a 218, comenzando después del prefiltro 211 y finalizando después del post-filtro 215. Como se discutió anteriormente, el generador de credenciales 201 inicial se puede colocar en el borde de la red 110 central, es decir, efectivamente en el extremo delantero del sistema de gestión de contenido general, especialmente en una realización de ejemplo de la invención distribuida (por ejemplo, como se muestra en la Figura 3 - elemento 201). Para cada instancia de un generador de credenciales, generalmente se proporciona una instancia del regenerador 219. En el ejemplo de instancia única que se muestra en la Figura 4, con solo una instancia tanto del generador de credenciales 201 como del regenerador 219, el regenerador 219 se coloca en el extremo, es decir, en la posición 228. La forma específica que se muestra en la línea sólida de la Figura 4 (es decir, un solo generador de credenciales en el extremo delantero y un solo regenerador en el extremo posterior) puede ser particularmente el caso si el sistema de gestión de contenido general se realiza sobre un dispositivo/entidad (por ejemplo, cuando cada proceso de submódulo puede estar utilizando una sola memoria compartida).

Sin embargo, cuando se utilizan múltiples regeneradores, cada regenerador debe operar antes de la siguiente instancia de un generador de credenciales (de modo que el regenerador puede mover los datos de contenido procesados desde el dominio etiquetado, genérico con generación de credenciales, de vuelta al dominio "normal", generalmente en el dominio misma especificación de tipo de archivo que el archivo electrónico de entrada original). Este ordenamiento específico de las instancias subsiguientes de generador de credenciales y regenerador se muestra mediante las flechas a las posiciones 222, 224 y 226 que están antes de las flechas a las posiciones 214, 216 y 218. Cuando se utilizan varias instancias del generador de credenciales/regenerador, esto proporciona un efecto de re-generación de credenciales entre cada subproceso.

Esta regeneración de credenciales tiene la ventaja, en cualquier implementación que utiliza una arquitectura de memoria compartida, para garantizar que no exista información de contenido obsoleto en la representación genérica etiquetada y, por lo tanto, permitir que se propague entre pasos al submódulo subsiguiente, porque cada paso comienza con los datos de contenido generación de credenciales 'nuevas' que se transformaron del archivo electrónico de entrada original. Considerando que, en una realización distribuida (como en la Figura 3), un solo generador de credenciales en el punto 212 puede ser todo lo que se requiere, ya que no puede haber ninguna posibilidad de que se mantengan datos obsoletos ya que cada proceso se realiza utilizando un hardware diferente (con diferente memoria). Más aún, con una arquitectura distribuida, puede haber una etapa de regeneración entre cada uno de los procesos mencionados anteriormente, y esta etapa de regeneración puede potencialmente generar la representación genérica etiquetada de los datos de contenido en un formato de archivo equivalente o igual como el archivo electrónico de entrada original (recordando que podemos generar un archivo de formato idéntico al del archivo electrónico de entrada (por ejemplo, pdf in, pdf out), o una forma diferente de archivo que pueda contener el mismo tipo de datos de contenido, por ejemplo, pdf in rtf out). Dicho de otra manera, el almacenamiento de memoria involucrado en el procesamiento es diferente.

La entidad 200 de gestión de contenido puede comprender además un motor 240 de ejecución que garantiza que una política de gestión de contenido seleccionada en vigor se aplique correctamente al archivo electrónico que pasa, por ejemplo, entre Internet 105 y la red 110 central. El motor de ejecución puede hacer esto controlando el funcionamiento de cada uno de los (sub)módulos de proceso dentro de los procesos 210 de gestión de contenido

general, es decir, en el ejemplo que se muestra, el módulo 211 de prefiltrado, módulo 213 de gestión de contenido, módulo 215 de filtro posterior, módulo 217 de validación y módulo 219 de regeneración.

Por ejemplo, los procesos 210 de gestión de contenido pueden llevar a cabo una transformación de los datos de entrada (por ejemplo, un archivo electrónico de Internet 105) a una representación genérica de ese archivo electrónico de entrada, a través de un proceso de regeneración de contenido que se describe con más detalle a continuación, que también puede incluir prefiltrado y posterior y una validación de dichos datos de contenido en una representación genérica con generación de credenciales. La determinación de qué datos de contenido deben regenerarse puede basarse en la toma de decisiones llevada a cabo por el motor 240 de ejecución (política de gestión de contenido). Es decir, el motor de ejecución puede estar dispuesto para proporcionar parámetros de política de gestión de contenido indicativos de, o para utilizar en la aplicación, la política de gestión de contenido que está vigente (es decir, que se está utilizando actualmente).

La entidad 200 de gestión de contenido puede comprender además un monitor 220 de parámetros de red acoplado operativamente al motor 240 de ejecución, para proporcionar de este modo parámetros de datos, tales como datos o parámetros de rendimiento de red inalámbrica, para el funcionamiento correcto del motor 240 de ejecución. Estos parámetros de rendimiento pueden ser, o incluir, parámetros operativos o de red derivados de la red 110 central y/o dispositivos 120-140 móviles.
Los parámetros utilizados/proporcionados por el monitor 220 de parámetros de red se pueden derivar de la red 110 central, desde, por ejemplo, la estructura 111 de conmutación CN (por ejemplo, en los cabezales de los paquetes de datos proporcionados por el hardware, tales como enrutadores y los conmutadores que forman dicha estructura 111 de conmutación CN), o se pueden derivar de un módulo o aplicación que opera dentro de los dispositivos 120-140 móviles conectados a la red 103 inalámbrica. En este último caso, los parámetros de red pueden proporcionarse al monitor 220 de parámetros de red mediante los dispositivos 120-140 móviles a través de un conector 230 de interfaz de usuario. Este conector 230 de interfaz de usuario se puede conectar a través de otro módulo, como el motor 240 de ejecución (como se muestra), o mediante una interfaz directa entre el conector 230 de interfaz de usuario y el monitor 220 de parámetros de red, no mostrado). Los datos para controlar los procesos 210 de gestión de contenido llevados a cabo por cualquiera de los módulos dentro de la entidad 200 de gestión de contenido mostrados en la Figura 4 se pueden almacenar en una base 260 de datos, que se puede acoplar operativamente a todos los módulos ya sea directa o indirectamente (por ejemplo, a través de una interfaz programática en el motor 240 de ejecución en el ejemplo que se muestra (es decir, no se muestran enlaces directos a cada módulo en esta Figura, para mayor claridad). La base 260 de datos puede residir dentro de la entidad 200 de gestión de contenido de instancia única, como se muestra en una línea continua, o puede estar ubicada fuera de la entidad 200 de gestión de contenido de instancia única, como se muestra en la base 260' de datos, contorno punteado. Esta última configuración de la base 260' de datos externa se puede utilizar particularmente con una instancia distribuida, con módulos 201 -204 separados (como se muestra en la Figura 3).

El motor 240 de ejecución de políticas puede basar su toma de decisiones en configuraciones de políticas almacenadas que se podrían almacenar en la base (260 o 260') de datos, tal como una base de datos de tipo SQL o cualquier forma de mecanismo de almacenamiento persistente. Las políticas almacenadas se pueden determinar por las entradas de datos del motor 220 de parámetros de red y/o el conector 230 de interfaz de usuario. El motor 240 de parámetros de red puede monitorizar el rendimiento de cualquier enlace de comunicaciones relevante (por ejemplo, los enlaces 114/115 de comunicaciones, o los enlaces 116 de comunicaciones inalámbricas entre cada dispositivo 120-140 móvil y la red 110 central, en las Figuras 1-3) en tiempo real, y puede ajustar las configuraciones de política del motor 240 de ejecución de políticas dependiendo de la calidad/rendimiento/etc. de dichos enlaces 114-116 de comunicaciones.

Por ejemplo, si un enlace 114-116 de comunicaciones particular es de una calidad deficiente, por ejemplo, determinada al medir la tasa de bits del enlace de comunicaciones o la relación señal a ruido durante un período de tiempo determinado (y potencialmente realizar un promedio continuo), entonces se puede determinar que la cantidad de datos de contenido que puede manejar ese enlace 114-116 de comunicación es menor. Por lo tanto, por ejemplo, la política determinada relacionada con el(los) dispositivo(s) móvil(es) conectado(s) a través de ese enlace 114-116 de comunicaciones de rendimiento más bajo se puede restringir (o restringir adicionalmente) de tal manera que se transfieran menos datos de contenido a través del respectivo enlace de comunicaciones de bajo rendimiento (mientras se reduce el rendimiento), y por lo tanto maximiza el ancho de banda útil. Este método mejora el rendimiento general de la red y puede mejorar la experiencia del usuario final. Por ejemplo, los datos del contenido del archivo electrónico que pueden enviarse a través del enlace pueden restringir la inclusión de texto e imágenes para incluir solo texto, o reducir la inclusión de video y audio, a solo audio, etc. Cuando el respectivo enlace de comunicaciones de bajo rendimiento vuelve a tener un rendimiento más alto, la restricción (o restricción adicional) se puede eliminar/reducir, según corresponda.

La política de gestión de datos de contenido aplicada por el motor 240 de ejecución puede comprender más de un aspecto, por ejemplo, puede comprender una retroalimentación en tiempo real basada en un aspecto automatizado, y un aspecto manual basado en, por ejemplo, limitaciones duras/fijas predefinidas. Por lo tanto, la política es totalmente ajustable para tener en cuenta los escenarios de uso, tanto a corto como a largo plazo.

El aspecto de política automatizada (por ejemplo, las configuraciones del motor de ejecución derivadas automática/por retroalimentación) se pueden disponer para tener prioridad sobre la configuración manual del usuario (como un todo o en un nivel más granular), o viceversa.

El aspecto de la política manual (por ejemplo, configuraciones del motor de ejecución manual) se puede proporcionar a través de la interfaz 230 de usuario desde los propios dispositivos de usuario, a través de la aplicación o módulo 104 o 204 móvil, como se muestra, o a través de Internet 105. También pueden estar, por lo menos parcialmente, preprogramados en el sistema en general, de tal manera que la interfaz de usuario es más un proceso de selección, en lugar de un proceso de definición complejo. Esta última disposición permite que se realicen políticas relativamente complejas con una mínima entrada/experiencia del usuario o incluso ancho de banda.

Se le puede permitir a un administrador o usuario general configurar las políticas de gestión de datos de contenido del motor 240 de cumplimiento en función de la capacidad de cualquier dispositivo móvil en uso en la red 103 inalámbrica, o con base en una postura de riesgo (es decir, una definición corporativa de un nivel de riesgo que están dispuestos a aceptar con su infraestructura de comunicaciones móviles, por ejemplo, pueden decidir no permitir nunca un documento de Word con macros). La postura de riesgo puede variar según el tiempo y la ubicación del dispositivo, y puede estar estrechamente relacionada con las políticas de seguridad de su organización o incluso con sus propias preferencias de usuario individuales. El conector 230 de interfaz de usuario se podría realizar como una aplicación de software central del lado de la red que se conecta con las aplicaciones o módulo (104 o 204) dedicado del lado móvil, o un módulo de hardware dedicado que reside dentro del dispositivo 120-140 móvil respectivo. Alternativa o adicionalmente, el sistema general puede proporcionar una interfaz de usuario integrada, como una interfaz basada en web, a la que se puede acceder a través de cualquier navegador web estándar (es decir, a través de Internet 105 en general).

La Figura 5 muestra un ejemplo, singular, de la conversión de un archivo 301 electrónico de entrada original a un archivo 301' electrónico de gestión de datos de contenido/modificado de salida singular, de acuerdo con un ejemplo de la invención. El archivo 301' electrónico de salida se puede denominar un archivo electrónico de salida con gestión de datos de contenido o con política restringida.

La conversión mostrada se puede llevar a cabo mediante la instancia singular de una entidad 200 de gestión de contenido (como se describe en la Figura 4), o se puede llevar a cabo por la versión de gestión de contenido distribuida pero funcionalmente similar (es decir, incluidos los módulos 201-204 descritos en la Figura 3).

El archivo 301 electrónico de entrada puede comprender cualquier selección adecuada de datos de contenido para el tipo de archivo particular del archivo electrónico de entrada y, por ejemplo, puede incluir datos de contenido tales como: texto 302 original, video 304 original, audio 306 original, Javascript 308, macro(s) 310 original(es), y Acroforms 312 originales. El término "original" utilizado en este documento es para decir los datos en la forma original antes de que se aplique cualquier gestión de datos de contenido (es decir, política) de acuerdo con ejemplos de la invención.

El archivo 301' electrónico de salida es uno en el que los procesos de gestión de contenido ahora se han aplicado, en base a, por ejemplo, la política de gestión de contenido aplicada por el motor 240 de cumplimiento, bajo la guía de los parámetros de datos almacenados en, por ejemplo, la base 260 de datos (como se muestra en la Figura 4).

Por lo tanto, el archivo 301' electrónico de salida puede comprender una nueva instancia predeterminada de contenido administrado, recientemente regenerado, de una selección de los datos de contenido originales del archivo 301 electrónico de entrada, para incluir (pero no limitado a), en el ejemplo que se muestra en la Figura 5, texto 302' gestionado por contenido, audio 306' gestionado por contenido y acroformes 312' gestionados por contenido. Por lo tanto, hemos reducido la cantidad de datos de contenido en el archivo 301' electrónico de salida, a solo la permitida por la política de gestión de datos de contenido actualmente vigente para el dispositivo de destino, y por lo tanto hemos reducido los requisitos de ancho de banda para el mismo, requisitos de procesamiento potencialmente reducidos, etc. pero lo que es más importante, se reduce la huella de riesgo de la entrega del archivo electrónico de entrada. Esto se debe a que el archivo 301' electrónico de salida ya no contiene datos de contenido indeseables o peligrosos, solo contiene datos de contenido bueno y permitido (porque es una nueva instancia de los datos de contenido del archivo recién regenerada, muy probablemente en una representación etiquetada genérica, solo utilizable por la aplicación/módulo 104 o 204 del lado del dispositivo móvil que se proporciona), de tal manera que no existe riesgo de infección por malware.

Los ejemplos de la invención también pueden proporcionar múltiples capacidades de conversión, es decir, la conversión de un archivo 301 electrónico de entrada original a múltiples instancias nuevas, diferentes, gestionadas por contenido de archivos 301' electrónicos de salida regenerados, para uso de diferentes dispositivos 120 móviles, de acuerdo con políticas diferentes (que a su vez se pueden basar en factores estáticos, tales como las capacidades respectivas del dispositivo móvil, o factores dinámicos, tales como el rendimiento/precio actual de la red inalámbrica, como se describe con más detalle en otra parte de esta descripción).

Por ejemplo, un solo archivo 301 electrónico de entrada puede contener conjuntos de datos de contenido originales: texto 302; video 304; audio 306; Javascript 308; Macros 310; Acroforms 312, y se convierte en un conjunto de diferentes archivos electrónicos de salida. Estos diferentes archivos electrónicos de salida pueden ser, por ejemplo:

Un primer archivo electrónico de salida que comprende: texto 302' gestionado por contenido; video 304' gestionado por contenido; y audio 306' gestionado por contenido.

Un segundo archivo electrónico de salida que comprende: texto 302' gestionado por contenido; video 304' gestionado por contenido; y audio 306' gestionado por contenido; Acroforms 312' gestionadas por contenido.

Un tercer archivo electrónico de salida que comprende solo texto 302' gestionado por contenido.

Un cuarto archivo de salida que comprende: texto 302' gestionado por contenido; video 304' gestionado por contenido; audio 306' gestionado por contenido; Javascript 308 gestionado por contenido; Macros 310 gestionados por contenido; Acroforms 312' gestionadas por contenido.

Los diferentes archivos electrónicos de salida, por ejemplo, los archivos electrónicos de primera a cuarta salida ejemplificados anteriormente, pueden proporcionarse a diferentes dispositivos móviles (cada uno con diferentes políticas de gestión de contenido aplicadas a ellos) y/o a los mismos dispositivos móviles a lo largo del tiempo (es decir, diferentes parámetros dinámicos vigentes. Por lo tanto, en los ejemplos anteriores, el primer archivo electrónico de salida puede proporcionarse a un dispositivo 130 de capacidad media con algunas restricciones en los datos de contenido (porque el dispositivo está en itinerancia); el segundo archivo electrónico de salida puede ser para proporcionar a un dispositivo 130 de capacidad media con menos restricciones en los datos de contenido (porque el dispositivo está en la red local); el tercer archivo electrónico de salida puede ser para proporcionar un dispositivo 120 de baja capacidad; y el cuarto archivo electrónico de salida puede ser proporcionado a un dispositivo 140 de alta capacidad con restricciones mínimas en los datos de contenido (porque el dispositivo cuenta con muchos recursos y en la red local, pero el malware nunca debería estar presente, por lo tanto, por lo menos una forma básica de gestión de contenidos antimalware).

La elección de qué políticas de gestión de datos de contenido (y, a su vez, restricciones) se aplican a cualquier dispositivo móvil dado que utiliza la red 103 inalámbrica es arbitraria, es decir, totalmente definible por la administración del sistema/parámetros de usuario vigentes y las condiciones de red experimentadas. Por lo tanto, la invención no se limita a ninguna combinación específica particular de políticas de gestión de datos de contenido.

La Figura 6 muestra un ejemplo de conversión (distribuida) de un archivo 301 electrónico de entrada original a un archivo 301' electrónico de salida de contenido gestionado singular, utilizando un archivo 301" electrónico intermedio, de acuerdo con un ejemplo de la invención. En una visión general, el ejemplo logra el mismo efecto general que la Figura 5, excepto que se realiza en una serie de etapas realizadas como una arquitectura distribuida de tal manera que el generador de credenciales 201, prefiltro 211, motor 213 de gestión de contenido, post-filtro 215, validación 217 de contenido y regenerador 219 no residen dentro de una entidad 200 de gestión de contenido singular sino como una multitud de entidades que se ubican a través de la red inalámbrica, por ejemplo, estructura de conmutación de red central, dispositivo móvil, etc. Los beneficios de llevar a cabo los procesos mencionados anteriormente en una serie de etapas en lugar de hacerlo en una sola entidad 200 de gestión de contenido son que permite que la infraestructura de red inalámbrica distribuya la carga de procesamiento a través de varios dispositivos de red para mantener el rendimiento. Las implementaciones distribuidas también pueden proporcionar cobertura para diferentes puntos de entrada dentro y fuera de la red 103 inalámbrica, potencialmente con diferentes políticas de gestión de contenido vigentes, de acuerdo el punto de entrada. Por ejemplo, una implementación puede tener una función/módulo de generador de credenciales que reside en el(los) teléfono(s) 120-140 móvil(es) (por ejemplo, dentro de la aplicación o módulo 104/204 del lado móvil), de tal manera que los datos de contenido que se envían desde el teléfono también se generan credenciales en preparación para el envío a través de la red 103 inalámbrica, y se procesa aún más como se describió en las secciones anteriores (es decir, prefiltrado/posterior, gestión de contenido, etc.). Mientras que el generador de credenciales 201 en la Figura 3 se muestra en un borde de la red, se deduce que el generador de credenciales, u otro ejemplo del mismo, puede residir (lógica o físicamente) en cualquier condición de borde de la red 110 central, incluso dentro del móvil. Dispositivos 120-140. Utilizar múltiples instancias/ubicaciones de dichos generadores de credenciales(es) permite, entonces, que se soporten múltiples conexiones con datos que también fluyen en múltiples direcciones.

El generador de credenciales 201 opera en el archivo 301 electrónico de entrada original, transformándolo en una representación etiquetada genérica que se discute a continuación en detalle. En el punto 303, el archivo electrónico de entrada ahora se ha convertido en un formato con generación de credenciales genérico. Parte del proceso del generador de credenciales 201, como se discute a continuación, puede ser un procedimiento básico de verificación de sintaxis en la representación genérica etiquetada de los datos del contenido original del archivo electrónico de entrada, lo que garantiza que la estructura básica de la representación genérica etiquetada del contenido original de los datos de contenido del archivo electrónico de entrada sea sintácticamente correcto. Al colocar el generador de credenciales 201 en el borde de la red 110 central, puede eliminar lo antes posible cualquier parte de (hasta e incluyendo todo) los archivos electrónicos de entrada que no cumplan con la política de gestión de contenido que se

está aplicando y, por lo tanto, reduzca el requisito de ancho de banda de la red 103 inalámbrica global (porque la red 103 inalámbrica ya no está enviando datos que no se pueden o no se deben utilizar). Más aún, esta eliminación de datos de contenido específicos en base a la política de gestión de contenido descrita, y que incluye un aspecto de seguridad al eliminar datos de contenido malformados/maliciosos, también significa que no hay pérdida de ancho de banda al enviar archivos electrónicos con formato incorrecto, o más importante, archivos electrónicos que contienen datos de contenido potencialmente maliciosos (por ejemplo, un virus, troyano, etc.). De esta manera, más del 90% del malware se puede detener en el punto inicial de entrada de los datos de contenido respectivos en la red inalámbrica, y especialmente en la red 110 central. Adicionalmente, como los datos del contenido del archivo electrónico de entrada ahora están en un formato de representación etiquetado genérico, es efectivamente inerte y no se puede utilizar realmente como malware a medida que avanza a través de otras etapas de procesamiento de la red inalámbrica, es decir, el motor 213 de gestión de contenido y el módulo 217 de validación de contenido, respectivamente.

La forma de representación etiquetada genérica de los datos de contenido del archivo electrónico de entrada original en 303 luego se puede procesar por el motor 213 de gestión de contenido, en el que las políticas predeterminadas se pueden aplicar al archivo electrónico de entrada dependiendo de los factores estáticos y automáticos/dinámicos descritos anteriormente. Esta etapa de procesamiento puede dar como resultado un archivo 301" electrónico intermediario (que se puede denominar una representación genérica etiquetada en otra parte de la descripción) que solo constituye partes permitidas de los datos del contenido original. El archivo 301" electrónico intermediario se puede procesar luego por el módulo 217 de validación de contenido, que aplica el conjunto de reglas predefinidas "bien conocidas" y solo permite la regeneración de los datos de contenido que se ajustan a dicho conjunto de reglas "bien conocidas".

Un aspecto adicional de los procesos de validación descritos puede incluir algunas "correcciones" o eliminación de datos de contenido que se realizarán bajo determinadas condiciones mediante el proceso 217 de validación de contenido. Por ejemplo, si un elemento 314" de imagen está contenido dentro del archivo 301" electrónico intermediario que no se ajusta a la regla de 'imagen' permitida para dichos datos de contenido para dicho tipo de archivo electrónico de entrada original, entonces este elemento de imagen se puede eliminar de la representación etiquetada genérica general durante esta etapa intermedia que resulta en un archivo 301' electrónico de salida que contiene solo todos los datos de contenido conformes/permitidos, y ninguno de los datos de contenido que no esté permitido por una decisión de política activa o no esté permitido debido a es una parte no conforme de los datos de contenido originales.

La Figura 7 muestra un método de gestión de contenido de acuerdo con un ejemplo de la invención, como se lleva a cabo por parte del hardware descrito anteriormente, o por ejemplo, como se muestra en las Figuras 4 y 5.

En una visión general, el método opera sobre un archivo 301 electrónico entrante, que generalmente contiene datos de contenido en una especificación de tipo de archivo predeterminada (y disposición asociada) correspondiente a un conjunto de reglas para dicho tipo de archivo (por ejemplo, recibir un archivo pdf, de acuerdo con una especificación del archivo pdf). El método puede comprender recibir 502 el archivo 301 electrónico entrante, luego realizar uno o más pasos sobre los datos de contenido dentro del archivo 301 electrónico de entrada, que puede incluir transformar los datos de contenido, en cada iteración, a una representación etiquetada genérica. El método también puede comprender realizar una o más de las funciones discretas de: generación de credenciales 504 del archivo electrónico entrante 301; prefiltro 506 (es decir, eliminación de 'ruido'); gestión 508 de contenidos; filtrado 510 posterior (es decir, limpieza del archivo antes de la salida); conformidad y validación 512 de dichos datos de contenido gestionados por contenido y generados con credenciales, filtrados (por ejemplo, contra un conjunto de límites razonables y buenos criterios); y tomando una decisión 514 de regeneración. En la que un 'sí' 515 para la decisión 514 de regeneración significa regenerar 516 los datos de contenido en un archivo electrónico de salida del mismo tipo que el archivo electrónico de entrada original, y en la que un 'no' 517 significa emitir los datos de contenido en una forma/formato 518 genérico etiquetado, para uso posterior en otra parte del sistema, o por otra entidad dentro del sistema general, todo en el dominio genérico.

Una característica potencialmente proporcionada por los ejemplos de la invención es la capacidad de corregir cualquier desviación frecuente del conjunto de reglas de validación, pero tal vez relativamente menor. Por ejemplo, cuando el texto debe tener avances de línea de texto y retornos de carro al final de cada línea nominal (cuando se ve), pero a menudo el texto se puede formar lentamente para utilizar solo el retorno de carro en tal caso. Otro problema similar puede ocurrir cuando los saltos de línea/retornos de carro en el texto dentro de un área de texto determinada se basan en las técnicas de "ajuste de texto" proporcionadas por el software de lectura/escritura, y por lo tanto no tienen caracteres de retorno de carro o control de tarifa de línea, como tal.

Cuando un ejemplo proporciona este tipo de característica correctiva, el motor de gestión de contenido se puede disponer de tal manera que estas 'correcciones' menores al formato de archivo se apliquen durante el proceso 213 de gestión de contenido. La característica de corrección generalmente tiene un alcance limitado, por lo tanto, el sistema se puede disponer para enumerar lo que se permitirá/podrá corregir (es decir, una "lista blanca" de corrección) y, por lo tanto, no se corrige nada fuera de este conjunto de correcciones permitido. Dicho de otra manera, el sistema solo puede corregir los errores básicos enumerados, conocidos anteriormente, que ocurren

comúnmente, y cualquier cosa externa que se considere demasiado extrema para la corrección automática. La lista de errores conocidos se puede actualizar en cualquier momento para reflejar datos más recientes, o un nivel de medida correctiva, es decir, el sistema se puede configurar para ser muy pedante o más permisivo.

Los submétodos 504-518 de componentes se describen con más detalle a continuación, bajo los encabezados respectivos.

El generador de credenciales

El proceso/submétodo 504 de generación de credenciales se lleva a cabo normalmente por el generador de credenciales 201, que se puede ubicar en múltiples puntos en el sistema general, como se describió anteriormente con referencia a la Figura 4, y de hecho se pueden utilizar múltiples instancias en algunos ejemplos (es decir, el generador de credenciales 201 se puede considerar un recurso común a cada uno de los otros procesos 210 de gestión de contenido).

El proceso 504 de generación de credenciales puede ser responsable de extraer datos de contenido del archivo 301 electrónico de entrada existente y representarlo en lo que llamamos anteriormente como una representación etiquetada/genérica. Esta representación genérica/etiquetada puede ser utilizada por otros submódulos/procesos (por ejemplo, módulo 211 de prefiltrado, módulo 213 de gestión de contenido, módulo 215 de posfiltrado, módulo 217 de validador, un módulo 219 de regenerador), de tal manera que estos submódulos subsiguientes no necesitan ser específicos del archivo, es decir, operan en el dominio etiquetado genérico, y como tales, pueden reutilizarse fácilmente para todas las formas de datos de contenido basados en archivos/tipo de archivo electrónico de entrada. Son archivos de tipo agnóstico. Esto proporciona eficiencias de procesamiento y gestión del sistema, especialmente la provisión de gestión de contenido a nuevas formas de archivo.

El proceso 504 de generación de credenciales puede tener un conjunto de mapeos predefinidos entre el archivo 301 electrónico de entrada y la representación etiquetada genérica. Es decir, cada archivo 301 electrónico de entrada tiene un mapeo entre cada subporción de datos de contenido del archivo electrónico de entrada y la porción respectiva de la representación etiquetada/genérica; por ejemplo, cómo se debe representar en el contenido binario y las etiquetas que se utilizan en dicha transformación. Por ejemplo, la porción 302 de texto original puede tener un mapeo a la forma con generación de credenciales de los datos del contenido del texto, la porción 304 de video original puede tener un mapeo a la forma con generación de credenciales de los datos del contenido de video, la porción 306 de audio original puede tener un mapeo a la forma con generación de credenciales de datos de contenido de audio, etc.

A continuación, se proporciona un ejemplo para resaltar cómo una representación de datos de contenido de texto original de un archivo 301 electrónico de entrada (el título de la pista/información del compositor de un archivo de música mp3, en este ejemplo) se puede colocar en una forma genérica etiquetada, mientras se transforma la totalidad del archivo electrónico de entrada (mp3) en la representación genérica general etiquetada.

Un archivo de música mp3 almacena datos codificados en binario en bloques y también tiene metadatos basados en cadenas (que incluye el texto) incorporados en el archivo electrónico mp3 en forma de etiquetas de datos ID3. Estas etiquetas normalmente se relacionan con la información textual relacionada con la música que se codifica dentro del archivo electrónico mp3, tal como (pero no limitado a): artista, género, derechos de autor, etc.

En el siguiente ejemplo, vemos que el proceso 504 de generación de credenciales ha transformado los datos de contenido originales (texto del título) del archivo 301 electrónico de entrada original en una representación etiquetada basada en generación de credenciales genérico de la etiqueta MP3 del compositor. En este caso, el proceso 504 de generación de credenciales tiene un mapeo entre la etiqueta de formato binario original “TCOM” de mp3 y una credencial genérica “glasswallTag: mp3TCOM” disponible y, por lo tanto, es capaz de transformar los datos de contenido de texto respectivos en esta representación genérica etiquetada, bajo el control de La política de gestión de contenidos actualmente vigente. Es decir, el proceso 504 de generación de credenciales toma los datos del contenido del texto original y los redispone en una forma genérica estandarizada para uso de una manera estandarizada, mediante el proceso/(sub)módulos subsiguientes.

En el registro de muestra etiquetado a continuación (es decir, en una forma con generación de credenciales o “credencial”), vemos que la etiqueta contiene los límites mínimo y máximo apropiados para los datos de este contenido de texto (que, en este ejemplo, es el campo del compositor de pistas), así como una entrada de la función de validación que puede ser llamada por el ciclo de validación más adelante, para validar este registro etiquetado. Esto permite que los registros individuales tengan una funcionalidad de validación única cuando sea apropiado.

<glasswallRecord: mp3TCOM>
representación = “texto restringido”
minLength = “1”
maxLength = “30”
valor = “ComposerX”

regenerar = “Sí”
validationFunction = “validateTcom”
</ glasswallRecord: mp3TCOM>

Tenga en cuenta que el campo de entrada ‘regenerar’ anterior se puede utilizar para determinar si se permite que este registro etiquetado (es decir, parte de los datos de contenido de texto) sea regenerado con base en la política de gestión de contenido actual. Si bien esto se presenta arriba en un contexto binario sí/no, puede comprender otros/más valores potenciales, por lo tanto, permitiendo que se aplique una disposición más matizada de los esquemas de regeneración. Este proceso 504 de generación de credenciales también puede ser responsable de realizar la comprobación de sintaxis básica discutida en la sección anterior, mientras analiza el archivo 301 electrónico de entrada y realiza la transformación del archivo electrónico de entrada original a la representación intermedia de generación de credenciales genérica del archivo 301”.

El ciclo de prefiltro

La etapa/método 506 de prefiltrado puede procesar el archivo con generación de credenciales, es decir, la representación genérica etiquetada creada por el proceso 504 de generación de credenciales descrito anteriormente, con el fin eliminar los datos de contenido que no están referenciados o no son accesibles al analizar el archivo 301 electrónico de entrada original (pero también se puede disponer para hacer similar dentro de la propia representación genérica etiquetada, también o en su lugar) utilizando un método de análisis predispuesto a medida de la entidad 200 de gestión de contenido/métodos 500 de ejemplos descritos de la invención (y puede, por ejemplo, utilizar un byte por byte, método lineal, o similar) en oposición al método de análisis recomendado estándar para el tipo específico de formato de entrada/especificación de archivo electrónico que se procesa (por ejemplo, el esquema de análisis pdf estándar aprobado conocido para un archivo pdf, el esquema de análisis Word documento(x) estándar aprobado conocido para un archivo doc(x), etc.). De esta manera, los aparatos y métodos de gestión de contenido descritos evitan ser subvertidos por un archivo 301 electrónico de entrada formado maliciosamente/formado incorrectamente que de lo contrario sería el caso de una función de lector normal. Más aún, este método significa que los datos de contenido que de otro modo podrían perderse con las técnicas de análisis estándar se tienen en cuenta, y se eliminan completamente si es necesario, sin dejar nada inesperado en el archivo 301’ electrónico de salida. El método descrito también se puede aplicar a una multitud de formatos/especificaciones de archivos de datos estructurados de manera diferente, que incluyen, pero no se limitan a, Microsoft Word(x), xls(x) y ppt(x), especificaciones de tipo de texto rtf (o texto similar más universal, especificaciones de tipo de archivo MP3/WAV (o audio similar más universal), y especificaciones de tipo de archivo.mp4/vob (o video similar más universal). Esencialmente, cualquier especificación de formato de tipo de archivo, para cualquier tipo de datos de contenido, puede tratarse con ejemplos de la invención, ya que se propagan a través de cualquier tipo de red inalámbrica, que incluyen, pero no se limitan a, mensajes de texto, correos electrónicos y tráfico web.

Los datos no referenciados o inalcanzables a menudo ocurren dentro de los archivos electrónicos que se transportan a través de redes inalámbricas, por ejemplo, cuando las aplicaciones que escriben archivos electrónicos realizan un “guardado rápido” y los datos se adjuntan al final del archivo electrónico y los datos obsoletos simplemente se dejan sin referencia (es decir, guardar rápido simplemente eliminó o cambió los punteros a los datos de contenido respectivos en el archivo electrónico “guardado rápido”, en lugar de eliminar los datos originales/volver a escribir el archivo electrónico sin los datos no referenciados en él). El proceso 506 de prefiltrado descrito es como una plantilla en la que se baja un lápiz imaginario para los datos de contenido a los que se hace referencia y se eleva para los datos de contenido que no están referenciados, de tal manera que, en una etapa de regeneración posterior, el uso de las etiquetas señaladas anteriormente (por ejemplo, la etiqueta de regeneración “sí/no”) los datos de contenido no referenciados se eliminan de manera efectiva. Este proceso 506 de prefiltrado elimina los datos de contenido superfluos no referenciados (que por su propia naturaleza no se requieren en ese archivo electrónico, y por lo tanto no se regeneran en la nueva instancia del archivo electrónico) al eliminar estos datos de contenido no referenciados en un primer paso de tal manera que cualquier módulo/submódulo de proceso adicional puede procesar la representación etiquetada genérica del archivo electrónico sin este ‘ruido’, que de otro modo podría resultar engañoso para los procesos adicionales de gestión de contenido y validación más adelante en la secuencia, o simplemente desperdiciar los recursos y ancho de banda de procesamiento utilizados posteriormente. Dicho de otra manera, la etiqueta “regenerar” se puede utilizar para determinar si los datos del contenido etiquetado particular se regenerarán nuevamente en la nueva instancia del archivo electrónico de salida, en la misma especificación de tipo de archivo que el archivo electrónico de entrada original (o Representación genérica etiquetada) o simplemente se deja atrás. Una vez más, todo el impulso con este método no es eliminar los datos de contenido incorrecto del archivo original (y, por lo tanto, dejar atrás los datos de contenido incorrecto que aún se desconocen), sino que solo se regeneran los datos de contenido que se sabe que son buenos y deseables, en el contenido del archivo electrónico de salida gestionado (es decir, sustituto).

El motor de gestión de contenido

La siguiente etapa en los procesos 210 de gestión de contenido puede ser la etapa 508 del método de gestión de contenido, que puede ser realizada, por ejemplo, por el módulo 213 de gestión de contenido. El motor de gestión de contenido puede verse como un ciclo de limpieza. La etapa 508 del método de gestión de contenido permite la

aplicación de políticas de gestión de contenido definidas por el administrador del sistema/usuario, que resulta de la configuración/decisiones de política automática y manual discutidas anteriormente (es decir, las porciones manuales de las cuales se han configurado previamente, y las porciones que están cambiando dinámicamente, por ejemplo, de acuerdo con las condiciones de la red, en este momento en el tiempo). La etapa 508 del método de gestión de contenido permite que los datos de contenido considerados indeseables (y por lo tanto no se regeneran) talas como, por ejemplo, Metadatos, JavaScript, Macros y Acciones Abiertas, se eliminen de la representación genérica etiquetada de los datos de contenido (y por lo tanto nunca lleguen al archivo 301' electrónico de salida final), antes de que los datos de contenido alcancen la etapa de regeneración.

Este método también tiene un beneficio adicional, ya que este ciclo de gestión de contenido también puede normalizar un documento o archivo 301 electrónico de entrada a una versión específica requerida (es decir, una versión actual o anterior predefinida de una especificación de tipo de archivo en constante cambio, por ejemplo, revisar una versión 1.4 de pdf recibida, hasta una versión 1.3 de pdf, en lugar de continuar utilizando pdf v1.4, o revisar desde .docx hasta .doc en Microsoft Word, etc.). Esto puede ser un beneficio particular cuando una versión más reciente de una especificación o formato de tipo de archivo tiene características que no son deseables (ya que agregan poco uso al flujo de trabajo de una organización, pero aumentan el impacto de la amenaza, por ejemplo, al contener una funcionalidad no utilizada que puede ser explotada de alguna manera).

Alternativamente, cuando una organización no se ha actualizado a la última versión del software en algunos dispositivos, pero sí en otros dispositivos, por ejemplo. software de productividad, tal como Microsoft Office, (por lo que el tipo de archivo más nuevo respectivo puede ser ilegible en las instalaciones más antiguas del software, debido a que el software de productividad preinstalado de algunos dispositivos móviles es una versión heredada), este problema de interoperabilidad se puede solucionar al utilizar el método de gestión de contenido descrito, porque el proceso general puede ignorar o revisar los datos de contenido o el tipo de datos de contenido que se introdujeron en una especificación de tipo de archivo más reciente que la especificación de tipo de archivo anterior, estandarizada y deseada.

El ciclo de postfiltro

El ciclo 510 de postfiltro se puede utilizar para garantizar que el ciclo 508 de gestión de contenido haya limpiado correctamente los datos de contenido general deseados de cualquier información de contenido no deseada y no haya dejado ningún enlace sin referencia. Este ciclo 510 de postfiltro tiene efectivamente la misma funcionalidad que el proceso 506 de prefiltrado, en el sentido de que cualquier enlace sin referencia o datos de contenido sin referencia se eliminan mediante un método de plantilla, pero se aplica después a diferencia de antes. El uso de instancias duales del filtrado proporciona una protección robusta contra la eliminación incompleta de datos de contenido no deseados, que de lo contrario podrían ocurrir si no se toma un método de eliminación iterativa (por ejemplo, en una estructura de árbol, en la que se hizo referencia originalmente a los datos de contenido de los niños, pero dependía de una porción/relación de los datos de contenido del padre, y los datos de contenido de los padres se eliminaron en el primer paso, por lo que la validez de los niños ha cambiado debido a la acción del primer paso de filtro). Dicho de otra manera, este método de filtrado iterativo se utiliza porque es engorroso y, en ocasiones, poco práctico para limpiar los datos de contenido de una representación genérica etiquetada de los datos de contenido de un archivo electrónico de entrada en un solo paso y los aparatos y métodos descritos efectivamente marcan los datos de contenido. como no se hace referencia en la etapa de gestión de contenido y luego simplemente "plantilla" los datos de contenido no referenciados en el ciclo 510 de postfiltrado.

El validador

Una etapa 512 de conformidad y validación, por ejemplo, llevada a cabo por el validador 217 en la Figura 4, es responsable de garantizar que los datos de contenido representados en la representación etiquetada genérica se ajusten a los límites predefinidos y las reglas aplicadas a esa forma de datos de contenido (por ejemplo, la longitud del límite de texto de campo, como se muestra en el ejemplo de MP3 anterior). Por ejemplo, en la muestra anterior, la etapa 512 de conformidad y validación puede inspeccionar los primeros tres campos y luego asegurar que el campo cuatro: <value = "ComposerX"> se ajuste al tipo y límites específicos establecidos anteriormente para estos datos de contenido, cuando se toman de una especificación de tipo de archivo mp3 como el archivo 301 electrónico de entrada. En el caso anterior, vemos que los datos de contenido en el campo 'valor' deben ser de tipo de texto restringido, lo que define un subconjunto de texto restrictivo y que la longitud del texto debe tener entre 1 y 30 caracteres. Si los datos de contenido en el campo 'valor' no se ajustan a estos criterios de bien conocido, entonces el registro no se regenera y se marca como tal en el campo 'regenerar' apropiado. La etapa 512 de conformidad y validación también puede tener alguna predefinición básica de límites y reglas de cumplimiento de datos de contenido generalmente permitidos o predeterminados, que pueden ser reemplazados o complementados por los límites y reglas predefinidos específicos de la especificación de tipo de archivo electrónico de entrada anotados anteriormente. El uso de dichos límites y reglas predeterminados puede ser particularmente útil cuando se encuentran otros tipos de archivos (por primera vez) aún no escuchados/encontrados/no soportados y se deben tratar de una manera rudimentaria, aunque solo sea para excluir finalmente sus datos de contenido enteramente.

La representación genérica etiquetada también puede tener una entrada para una función de rutina de validación a la que llamará el validador; esto puede proporcionarse específicamente (para cada especificación de tipo de archivo que puede ser manejada por los aparatos y los métodos descritos) rutina de validación, o una rutina de validación más aplicable genéricamente, o de hecho cualquier función que pueda considerarse útil en cualquier situación dada. Esto permite que el proceso genérico se adapte y amplíe para adaptarse a una funcionalidad específica que no se ajuste a una categoría de validación simple tal como texto o caracteres, o simplemente se puede utilizar para notificar al sistema (o a los administradores del mismo) del tipo de datos de contenido, tipo(s) de archivos o funcionalidad recientemente encontrados.

Un beneficio adicional de tener una funcionalidad de validación específica de tipo de archivo discreto por separado y de colocar la rutina 512 de validación como el último proceso de ejecución, es que si algún error de implementación ha provocado que el proceso de gestión de contenido no limpie o desinfecte correctamente una porción de los datos de contenido, entonces la rutina 512 de validación posterior será capaz de recogerlo en su lugar. Por ejemplo, debido a que esa porción no deseada de los datos de contenido no se encuentra en su lista de bien conocidos.

El regenerador

El regenerador 219, o cualquiera de las (múltiples) instancias del mismo, analiza la representación con generación de credenciales, es decir genérica etiquetada de los datos de contenido, es decir, crea una nueva instancia sustituta, recién generada, de un archivo electrónico de gestión por contenido con salida, ya sea en el mismo o similar formato al archivo 301 electrónico de entrada original (por ejemplo, convertir un archivo pdf de entrada en un archivo de salida pdf regenerado, o convertir un archivo pdf de entrada en un archivo de salida pdf de la versión inferior, etc.), o emitir los datos de contenido en otra forma de archivo de salida específico (por ejemplo, la conversión de un archivo pdf de entrada en un archivo de salida.doc de Word regenerado). Efectivamente, este proceso es el inverso del generador de credenciales 201 y mientras que el generador de credenciales 201 tiene un mapeo (por ejemplo, la disposición de la tabla de consulta) entre los datos de contenido del archivo electrónico original y las etiquetas adecuadas para representar dichos datos de contenido en la representación etiquetada genérica en el dominio etiquetado/generado con credenciales, el regenerador puede tener el mapeo inverso, es decir, un mapeo entre la forma de representación etiquetada genérica/con generación de credenciales de las etiquetas, con aquella de las porciones de datos del contenido del archivo electrónico original.

Alternativamente, el archivo 301' electrónico de salida puede de hecho permanecer como una representación etiquetada genérica, de tal manera que el procesamiento adicional puede ser armonizado/hecho más eficiente. Por ejemplo, el cifrado, la compresión y otras funciones de procesamiento pueden funcionar mejor, si pueden saber exactamente dónde se encuentra cada tipo de porción de datos de contenido, para todas las diferentes especificaciones de tipo de archivo que pueden ser manejadas por los aparatos y métodos descritos y actuar de acuerdo con lo anterior. Mientras que, si la misma función de procesamiento tiene que ver con diferentes tipos de archivos específicos y, por lo tanto, diferentes formas de datos de contenido y ubicaciones dentro de esos tipos de archivos, las funciones de procesamiento adicionales se vuelven más complejas de implementar y/o difíciles de crear, administrar y aplicar. Básicamente, las funciones de procesamiento adicionales (posteriores) (de cualquier tipo) se vuelven más eficientes si sus datos de entrada son más consistentes.

Tomando el ejemplo específico del dispositivo móvil, esto permitiría una forma genérica única de aplicación de lector hecha a la medida sobre un dispositivo móvil, por ejemplo, proporcionado dentro de la aplicación/módulo 104 o 204 del dispositivo móvil, para tratar (por ejemplo, procesar o incluso escribir) cualquier especificación de tipo de archivo, en lugar de necesitar una multitud de lectores diferentes, y actualizaciones para los mismos. Dicho de otra manera, la carga de transformación de la conversión del archivo 301 electrónico de entrada original (es decir, la transformación en el formulario de representación etiquetado genérico) se puede colocar en la red 103 inalámbrica (o incluso en la red 110 central del mismo), en lugar del dispositivo 120-140 móvil en sí mismo. Como resultado, la infraestructura 110 de red ha realizado la tarea de determinar los datos de contenido permitidos, así como representar los datos de contenido en forma genérica. Por lo tanto, los dispositivos 120, 130 y 140 móviles, pueden tener que ocuparse de la representación de datos de contenido de un formato de representación genérico singular, por ejemplo, sobre su pantalla. Como resultado, ya no les preocupa el formato de especificación de tipo de archivo específico del archivo 301 electrónico original y todas las múltiples combinaciones del mismo. Esto evita que el dispositivo móvil requiera una multitud de lectores/analizadores para la gran cantidad de datos de contenido en diferentes formas del archivo 301 electrónico de entrada y ahora el dispositivo móvil solo requiere un lector singular: el de la representación etiquetada genérica.

La Figura 10 describe un ejemplo más específico que detalla cómo se pueden almacenar los datos del contenido del archivo electrónico entre y durante cada uno de los procesos mencionados anteriormente procesos 506 de prefiltrado, gestión 508 de contenido, postfiltro 510; y ciclo 512 de conformidad y validación del contenido. El archivo 301 electrónico de entrada se lee en un almacenamiento 702 de memoria de entrada para que pueda leerse de forma rápida y contigua para la siguiente etapa, 704, que es una etapa de almacenamientos de contexto que se ocupa de generar de credenciales el archivo en la representación genérica etiquetada (como se discutió anteriormente), con una forma intermedia procesada por los almacenamientos 706 intermedios que realizan el proceso de prefiltrado, como se discutió anteriormente. Una diferencia clave con este ejemplo es que regenera la

representación genérica etiquetada de los datos del contenido del archivo de entrada original en su forma original, utilizando el almacenamiento 708 de salida en la salida de cada etapa (506, 508, 510, 512) de procesamiento para garantizar que los datos de contenido obsoletos, en forma de generación de credenciales, no se les permite, de manera involuntaria, pasar a los procesos posteriores. Al regenerar los datos del contenido del archivo y luego volver a la generación de credenciales en cada etapa, se puede garantizar que los datos del contenido son datos de contenido "nuevos" como resultado del último ciclo de procesamiento y no de algunos datos de contenido heredados de una serie de ciclos de procesamiento anteriores Este ejemplo particular puede ser relevante para una situación en la que el motor 210 de gestión de contenido no está distribuido, pero está concentrado en una única ubicación o dispositivo físico, como la entidad 200 de gestión de contenido en la Figura 2. Cuando se distribuye el motor 210 de gestión de contenido, como se describe en la Figura 3, esta regeneración en cada etapa puede no ser necesaria. Esto se debe a que se puede garantizar que cada proceso tenga datos 'nuevos' porque solo realiza un proceso único en oposición a todos los procesos a la vez, con la misma memoria.

La Figura 8 muestra una porción del método de ejemplo de la Figura 7 con más detalle, y cómo se utilizan en particular los diferentes almacenamientos de memoria. Este ejemplo muestra un caso en el que hay un generador de credenciales y un regenerador aplicados en cada etapa del submódulo, es decir, hay un generador de credenciales en cada una de las posiciones 212, 214, 216 y 218 en la Figura 4, y un regenerador en cada una de las posiciones 222, 224., 226 y 228. La porción de ejemplo que se muestra comprende, después de la entrada inicial del archivo 301 electrónico, cuatro ciclos: ciclo 0 a ciclo 3.

El ciclo 0 es el ciclo 506 de prefiltro, y se muestra que comprende una carga de almacenamientos de memoria de entrada del archivo electrónico de entrada; esto se puede hacer, por ejemplo, al cargar los datos del contenido del archivo en un almacenamiento de RAM, que permite un acceso rápido a los datos de contenido por/para los posteriores subprocesos adicionales que se tratan en breve. Los datos en los almacenamientos 702 de memoria pueden luego ser generados de credenciales, utilizando el generador de credenciales 201, como se describió anteriormente, cuya salida se almacena en un almacenamiento 704 de contexto de credenciales. El proceso 211 de prefiltro se realiza luego sobre la representación genérica de los datos de contenido, en el almacenamiento 704 de memoria de contexto, con los datos de contenido resultantes almacenados en la memoria 706 de almacenamiento intermedia. Luego, finalmente (para este submódulo), los datos de contenido se pueden regenerar en la forma de especificación de tipo de archivo electrónico original (por ejemplo, pdf) utilizando el almacenamiento 708 de memoria de salida, o alternativamente la representación genérica se copia simplemente a este almacenamiento 708 de memoria de salida, en preparación para el siguiente ciclo/proceso, cuando no se utiliza realmente ningún regenerador al final del proceso 506 de submódulo del prefiltro (es decir, los datos se mantienen en la forma de representación de generación de credenciales etiquetada genérica hasta el final).

El siguiente ciclo, ciclo 1, es el ciclo 508 de gestión de contenido (que puede, y en este caso, incluye un proceso de limpieza). En este documento, los datos electrónicos almacenados en la etapa anterior en el almacenamiento 708 de salida se copian en el almacenamiento 710 de memoria de entrada para la siguiente etapa 508, efectivamente, un intercambio de almacenamiento de memoria, en el que luego se generan credenciales, si es necesario, utilizando el generador de credenciales 201, en (otro o el mismo) almacenamiento 712 de contexto de credencial. El proceso 213 de gestión de contenido se aplica luego a los datos de contenido en el almacenamiento 712 de memoria de contexto, y con base en los parámetros estáticos o dinámicos detallados anteriormente, los datos de contenido gestionados por contenido resultantes se almacenan en el almacenamiento 714 de memoria intermedia, en el que se puede aplicar un proceso de limpieza, un proceso de limpieza de corrección semántica en este ejemplo (pero otras correcciones, como se discutió anteriormente, dentro de los límites, también se contemplan para uso en este punto del proceso general). El regenerador 219 puede luego regenerar los datos del contenido del archivo electrónico en el almacenamiento de memoria de salida 716, ya sea en el formato de archivo electrónico original (es decir, la regeneración adecuada) o en la representación genérica (una función de transferencia de datos de solo copia).

El ciclo 2 es el proceso 215 de postfiltro, y puede comprender cargar la representación electrónica de 716 en el almacenamiento 718 de memoria de entrada para esta etapa. Nuevamente, esto puede ser un simple intercambio de datos en el almacenamiento de memoria, o incluso un intercambio de nombre/direccionamiento del almacenamiento de memoria. El generador de credenciales 201, luego puede transformar la representación electrónica de los datos de contenido procesados hasta el momento en una representación genérica, etiquetada, utilizando el almacenamiento 720 de almacenamiento de memoria de contexto. El proceso de postfiltro luego se puede aplicar a la representación electrónica en el almacenamiento 720 de memoria de contexto, con los datos de contenido procesados (postfiltrados, en este caso) resultantes que se escriben en el almacenamiento 722 de memoria intermedia. A partir de este almacenamiento 722 de memoria intermedia, el contenido de datos está entonces o bien se regenera de nuevo a la especificación de tipo archivo electrónico original (o equivalente funcional, tal como otra especificación del tipo de archivo adecuado para el tipo de datos de contenido que se les permita en el sistema) o es de salida en su forma de representación genérica etiquetada al almacenamiento 724 de memoria intermedia de salida.

El ciclo final es el ciclo 3. Este es un ciclo 512 de validación, que lee los datos de contenido prefiltrado, gestionados por contenido y post-filtrado desde el almacenamiento 724 de memoria de salida y almacena este en un almacenamiento 726 de memoria de entrada para esta etapa (de nuevo al intercambiar los almacenamientos de

memoria de entrada/salida en el ejemplo mostrado en la Figura 8). El generador de credenciales 201 puede transformar los datos de contenido en una representación genérica y almacenar esto en un almacenamiento 728 de memoria de contenido. El validador 217 puede entonces realizar las rutinas de validación como se describió anteriormente, y los datos de contenido filtrados y gestionados por contenido validados resultantes se escriben en el almacenamiento 730 de memoria intermedia. Por último, el regenerador da salida a los datos de contenido ahora completamente procesados, ya sea en una representación genérica etiquetado, o en la especificación de tipo de archivo electrónico (u objetivo de conversión) original utilizando el almacenamiento 732 de memoria de salida, listo para ser comprometido en el disco como el archivo 301' electrónico de salida.

En la descripción anterior de la Figura 8, un solo almacenamiento (por ejemplo, almacenamiento de memoria de entrada, almacenamiento de memoria de contexto, almacenamiento de memoria intermedia, etc.) se describe en cada paso, pero como se muestra en las Figuras, puede haber múltiples almacenamientos de memoria utilizados para cada uno, depende de la arquitectura de la memoria y/o la forma de datos de contenido (por ejemplo, tamaño, etc.). Puede haber un solo almacenamiento de memoria utilizado por el tipo de datos de contenido que se procesa, por ejemplo, un almacenamiento de memoria para audio, otro almacenamiento de memoria para video, etc.

Como se describió anteriormente, la especificación de tipo de archivo utilizada en diferentes puntos del proceso de gestión de contenido general puede cambiar, es decir, se puede utilizar otra especificación de tipo de archivo cuando es más adecuada para el tipo de datos de contenido que se permiten a través del sistema. En la forma más simple, esto permite la conversión de una especificación de tipo de archivo de entrada a otra especificación de tipo de archivo de salida o intermedia (por ejemplo, una conversión de Microsoft Word.doc a un Formato de texto más rico.rtf más genérico). Sin embargo, en escenarios de implementación más complejos, una conversión puede ser más importante, ya que un archivo se convierte a medida que los datos de contenido no están permitidos. Por ejemplo, un archivo pdf de entrada con imágenes, audio, enlaces y el texto se puede convertir en un archivo de imagen simple para sólo los datos de contenido de imagen. es decir, cuando los datos de contenido no son permitidos, y por lo tanto ya no se incluyen en las versiones regeneradas (y por lo tanto efectivamente "despojados", la salida y/o archivo electrónico intermedio utilizado puede ser una especificación de tipo de archivo menor que no es capaz de incluir el contenido de datos no permitidos, ya que ya no es necesario el uso de una especificación de tipo de archivo que pueda contener los datos de contenido no permitidos.

La invención también se puede implementar como un producto de programa informático que se ejecuta en un aparato programable que comprende uno o más procesadores que operan dentro de, por ejemplo, un sistema informático, como entidad 200 de gestión de contenido, dicho producto de programa de ordenador que incluye por lo menos porciones de código ejecutable dispuestas para realizar una o más etapas de cualquier método de acuerdo con ejemplos de la invención cuando se ejecute en el aparato programable, tal como el sistema de ordenador. Se pueden incorporar ejemplos como el firmware almacenado dentro de, o por lo menos accesible por, hardware adecuado, tal como hardware de red, que incluye hardware de red inalámbrico tal como, pero no limitado a dispositivos móviles para conexión a una o más redes inalámbricas. Las redes inalámbricas que se pueden utilizar en ejemplos de la invención incluyen redes inalámbricas tanto terrestres como basadas en satélites.

Un producto de programa informático puede estar formado por una o más instrucciones que son ejecutables por uno o más procesadores, o por subporciones de los mismos, tales como núcleos de procesamiento, coprocesadores o similares. El producto de programa informático puede comprender un programa de aplicación específico y/o una porción de un sistema operativo global. El producto de programa informático puede incluir, por ejemplo, uno o más de: un servidor o servlet, un método de objeto, una función, un procedimiento, un objeto, una subrutina, una aplicación ejecutable, una aplicación o applet, código fuente o porción del código fuente, un código de objeto, una biblioteca compartida/vinculada/biblioteca de carga dinámica y/o cualquier otra secuencia de microcódigo, llamadas de función o conjunto de instrucciones diseñadas para ejecutarse sobre uno o más recursos de procesamiento adecuados, tales como procesadores, núcleos de procesamiento) o unidad(es) de procesamiento.

El programa informático puede almacenarse en cualquier medio de almacenamiento convenientemente dispuesto y accesible por dicho uno o más recursos de procesamiento, que pueden incluir medios de almacenamiento volátiles o no volátiles, por ejemplo, pero no limitado a: medios de almacenamiento óptico (por ejemplo, CD-ROM, DVD, Blue Ray, et al), RAM (por ejemplo, RAM dinámica, RAM estática, RAM no volátil, etc.), medios de almacenamiento magnético (por ejemplo, como unidades de disco duro, cintas magnéticas, etc.), etc. Los ejemplos que implementan aspectos de la invención no están limitados a su forma específica, sino que están limitados solo por la funcionalidad para almacenar datos para su manipulación y/o controlar dicha manipulación de los mismos datos, similares o diferentes. Los medios de almacenamiento también pueden comprender almacenamiento conectado a la red, y pueden incluir tecnologías de almacenamiento basadas en la nube; para incluir cualquier medio de almacenamiento de datos mantenido de manera diversa, que en sí mismos puede comprender o por lo menos incluir bases de datos, instancias de bases de datos, bases de datos separadas lógica y/o físicamente y similares. El rango completo de tecnologías de almacenamiento de datos disponibles ahora o creadas en el futuro, están previstas para uso con por lo menos un ejemplo de la presente invención. Los medios de almacenamiento previstos también incluyen cualquier tecnología de transmisión adecuada, de tal manera que una onda de transmisión o una onda EM similar también se pueda utilizar para almacenar datos, por lo menos transitoriamente.

En la especificación anterior, la invención se ha descrito con referencia a ejemplos específicos de realizaciones de la invención. Sin embargo, será evidente que se pueden realizar varias modificaciones y cambios sin apartarse del alcance más amplio de la invención como se expone en las reivindicaciones adjuntas.

Cualquier forma de conexión discutida en este documento, por ejemplo, cuando una entidad se describe como acoplada/conectada operativamente a otra, puede ser cualquier tipo de conexión(s) adecuada(s) para transferir datos que transportan señales desde o hacia dichas entidades, unidades o dispositivos, y puede incluir el envío de datos que transportan señales a través de entidades, unidades o dispositivos intermedios. De acuerdo con lo anterior, a menos que se indique lo contrario o esté implícito, las conexiones pueden incluir una o más de: conexiones directas; conexiones indirectas; una sola conexión; una pluralidad de conexiones, conexiones bidireccionales; conexiones unidireccionales. Las conexiones pueden operar de cualquier manera que permita la transferencia de datos entre puntos terminales o, de hecho, nodos a lo largo de la longitud de la(s) conexión(es), por ejemplo, en serie, en paralelo o de forma multiplexada (por ejemplo, multiplexada por tiempo, frecuencia, fase, etc.).

Aquellos expertos en la técnica reconocerán que los límites entre los diferentes bloques lógicos, bloques de circuitos o entidades descritos en este documento son solo ilustrativos y que los ejemplos alternativos pueden combinar bloques lógicos, bloques de circuitos o elementos de entidad o utilizar una o más descomposiciones alternativas de funcionalidad en varias lógicas. Bloques, bloques de circuitos o elementos de entidad. Por lo tanto, se debe entender que las arquitecturas de procesamiento representadas en este documento se exponen simplemente como un ejemplo, y en su lugar se pueden utilizar disposiciones funcionales similares.

Cualquiera de los límites descritos en los ejemplos específicos presentados en este documento, son solo ilustrativos. Cualquier operación descrita, incluyendo múltiples operaciones discretas, de hecho, puede combinarse en una sola operación, igualmente una operación única puede de hecho distribuirse para formar suboperaciones adicionales y dichas operaciones/suboperaciones se pueden ejecutar por lo menos parcialmente solapándose en el tiempo, dependiendo de los tiempos requeridos de la o cada entidad (o entidades) dentro del sistema ejemplar global descrito.

Sin embargo, también son posibles otras modificaciones, variaciones y alternativas. De acuerdo con lo anterior, las especificaciones y los dibujos se deben considerar en sentido ilustrativo en lugar de restrictivo.

REIVINDICACIONES

1. Un aparato (200) de gestión de datos de contenido móvil antimalware, para uso en gestión de datos de contenido dentro de un archivo electrónico de entrada que contiene datos de contenido para ser enviados a través de una red inalámbrica que sirve por lo menos a un dispositivo móvil, que comprende:

por lo menos un generador de credenciales (201) para generar de credenciales los datos de contenido incluidos dentro del archivo electrónico de entrada en una representación genérica etiquetada de los datos de contenido;

un motor (213) de gestión de contenido para aplicar una política de gestión de contenido predeterminada a la representación genérica etiquetada de los datos de contenido para formar datos de contenido genéricos etiquetados gestionados por contenido; y

un validador (217) para crear datos de contenido gestionados por contenido validados al ser dispuestos para asegurar los datos de contenido gestionados por contenido representados en la representación genérica etiquetada gestionada por contenido se ajuste a cualesquier limites predefinidos y reglas aplicadas a cada forma de datos de contenido que aparece en los datos de contenido del archivo electrónico de entrada;

en el que el validador se acopla operablemente a la red inalámbrica, y se dispone a emitir un archivo electrónico de salida sustituto derivado de los datos de contenido gestionados por contenido validados;

en el que el aparato de gestión de datos de contenido móvil comprende adicionalmente un motor (240) de ejecución acoplado operablemente al motor de gestión de contenido y dispuesto para proporcionar parámetros de política de gestión de contenido indicativos de, o para uso en aplicar, la política de gestión de contenidos que estará vigente;

en el que el aparato de gestión de datos de contenido móvil comprende adicionalmente un monitor (220) de parámetros de red acoplado operablemente al motor de ejecución y dispuesto para proporcionar parámetros de red al motor de ejecución, para su uso en la configuración o modificación de los parámetros de política de gestión de contenido; y

en el que el monitor (220) de parámetros de red se dispone para monitorizar el desempeño de los enlaces (114-116) de comunicación en uso sobre la red inalámbrica en tiempo real, y para ajustar la configuración de políticas del motor (240) de ejecución que dependen de la calidad o desempeño de los enlaces (114-116) de comunicación.

2. El aparato (200) de gestión de datos de contenido móvil antimalware de la reivindicación 1, que comprende adicionalmente por lo menos un filtro (211, 215) para filtrar la representación genérica etiquetada de los datos de contenido para eliminar datos de contenido no referenciados o inalcanzables.

3. El aparato (200) de gestión de datos de contenido móvil antimalware de la reivindicación 1, en el que el aparato de gestión de datos de contenido móvil comprende adicionalmente un conector de interfaz de usuario acoplado operablemente al motor de ejecución y dispuesto para proporcionar parámetros de política de gestión de contenido desde por lo menos uno de: por lo menos un dispositivo móvil que es servido por la red inalámbrica, la red inalámbrica en sí misma, o un usuario de por lo menos un dispositivo móvil que es servido por la red inalámbrica.

4. El aparato (200) de gestión de datos de contenido móvil antimalware de la reivindicación 1, en el que los parámetros de política de gestión de contenido se derivan de información con base en ubicación proporcionada desde un sensor de ubicación dentro de por lo menos un dispositivo móvil o dentro de una entidad de red inalámbrica que sirve en por lo menos un dispositivo móvil.

5. El aparato (200) de gestión de datos de contenido móvil antimalware de la reivindicación 1, en el que por lo menos un generador de credenciales comprende múltiples generadores de credenciales en diferentes ubicaciones dentro del motor de gestión de contenido, cada uno dispuesto para volver a generar de credenciales los datos de contenido antes de una etapa de procesamiento posterior.

6. El aparato (200) de gestión de datos de contenido móvil antimalware de la reivindicación 1, en el que el aparato de gestión de datos de contenido móvil es un aparato de gestión de datos de contenido móvil distribuido que tiene submódulos dispuestos para llevar a cabo etapas de procesamiento en diferentes ubicaciones dentro de la red inalámbrica.

7. El aparato (200) de gestión de datos de contenido móvil antimalware de la reivindicación 1, en el que el aparato de gestión de datos de contenido móvil es un aparato (200) de gestión de datos de contenido móvil de única instancia, y la única instancia comprende adicionalmente por lo menos un segundo filtro para filtrar la representación genérica etiquetada de los datos de contenido para eliminar datos de contenido no referenciados o inalcanzables después de que el motor de gestión de contenido ha aplicado una política de gestión de contenido predeterminada a una representación genérica etiquetada filtrada de los datos de contenido.

8. Un sistema que comprende el aparato (200) de gestión de datos de contenido móvil antimalware de cualquiera de las reivindicaciones 1 a 7 y un dispositivo (120, 130, 140) móvil que comprende una aplicación (204) lateral del dispositivo móvil configurada para uso con el aparato (200) de gestión de datos de contenido móvil antimalware, en el que la aplicación (204) lateral del dispositivo móvil comprende una función de lector genérico para permitir el uso y/o manipulación de los datos de contenido incluidos dentro de cualquier instancia de representación genérica etiquetada de los datos de contenido, y una porción de la consola de gestión operable para permitir un usuario del dispositivo móvil para configurar o modificar la política de gestión de contenido que se va a aplicar al mismo dispositivo móvil, u otros dispositivos móviles servidos por la red inalámbrica.

9. Un método (500) de gestión de datos de contenido móvil antimalware, para uso en gestionar por contenido un archivo electrónico de entrada que contiene datos de contenido para ser enviados a través de una red inalámbrica que sirve por lo menos a un dispositivo (120, 130, 140) móvil, el método comprende:

generar de credenciales (504) los datos de contenido incluidos dentro del archivo electrónico de entrada en una representación genérica etiquetada de los datos de contenido;

gestionar por contenido (508) la representación genérica etiquetada de los datos de contenido para aplicar una política de gestión de contenido predeterminada a la representación genérica etiquetada de los datos de contenido para formar datos de contenido gestionados por contenido;

validar (512) los datos de contenido gestionados por contenido representados en la representación genérica etiquetada para asegurar que dichos datos de contenido gestionados por contenido se ajusten a cualesquier limites predefinidos y reglas aplicadas a cada forma de datos de contenido que aparece en los datos de contenido del archivo electrónico de entrada, para formar datos de contenido gestionados por contenido validados; y

emitir (518) un archivo electrónico de salida sustituto derivado de los datos de contenido gestionados por contenido validados;

en el que el método comprende adicionalmente:

proporcionar parámetros de política de gestión de contenido indicativos de, o para uso en aplicar, la política de gestión de contenidos que estará vigente a través de un motor de ejecución acoplado operablemente al motor de gestión de contenido;

proporcionar parámetros de red al motor de ejecución a través de un monitor de parámetros de red acoplado operablemente al motor de ejecución, con el fin de proporcionar medios para configurar o modificar los parámetros de política de gestión de contenido;

monitorizar el desempeño de los enlaces (114-116) de comunicación en uso sobre la red inalámbrica en tiempo real; y

ajustar los parámetros de políticas que dependen de la calidad o desempeño de los enlaces (114-116) de comunicación.

10. El método (500) de gestión de datos de contenido móvil antimalware de la reivindicación 9, que comprende adicionalmente filtrar (506) la representación genérica etiquetada de los datos de contenido para eliminar datos de contenido no referenciados o inalcanzables.

11. El método (500) de gestión de datos de contenido móvil antimalware de la reivindicación 9, que comprende adicionalmente proporcionar parámetros de política de gestión de contenido, a través de un conector de interfaz de usuario acoplado operablemente al motor de ejecución, desde por lo menos uno de: por lo menos un dispositivo (120, 130, 140) móvil que es servido por la red inalámbrica, la red inalámbrica en sí misma, o un usuario de por lo menos un dispositivo móvil que es servido por la red inalámbrica.

12. El método (500) de gestión de datos de contenido móvil antimalware de la reivindicación 11, que comprende adicionalmente derivar los parámetros de política de gestión de contenido a partir de la información con base en ubicación proporcionada por un sensor de ubicación dentro de por lo menos un dispositivo (120, 130, 140) móvil o dentro de una entidad de red inalámbrica que sirve por lo menos un dispositivo (120, 130, 140) móvil.

13. El método (500) de gestión de datos de contenido móvil antimalware de la reivindicación 9, que comprende adicionalmente proporcionar múltiples generadores de credenciales en diferentes ubicaciones dentro del motor de gestión de contenido, cara uno dispuesto para volver a generar de credenciales los datos de contenido antes de una etapa de procesamiento posterior.

14. El método (500) de gestión de datos de contenido móvil antimalware de la reivindicación 9, que comprende adicionalmente distribuir submódulos del aparato de gestión de datos de contenido móvil a través de diferentes

ubicaciones dentro de la red inalámbrica, cada submódulo se dispone para llevar a cabo una etapa de procesamiento diferente de un proceso de gestión de contenido general.

15. El método (500) de gestión de datos de contenido móvil antimalware de la reivindicación 9, que comprende adicionalmente por lo menos una segunda etapa de filtro (510) para filtrar la representación genérica etiquetada de los datos de contenido para eliminar datos de contenido no referenciados o inalcanzables después de que el motor de gestión de contenido ha aplicado una política de gestión de contenido predeterminada a una representación genérica etiquetada filtrada de los datos de contenido.

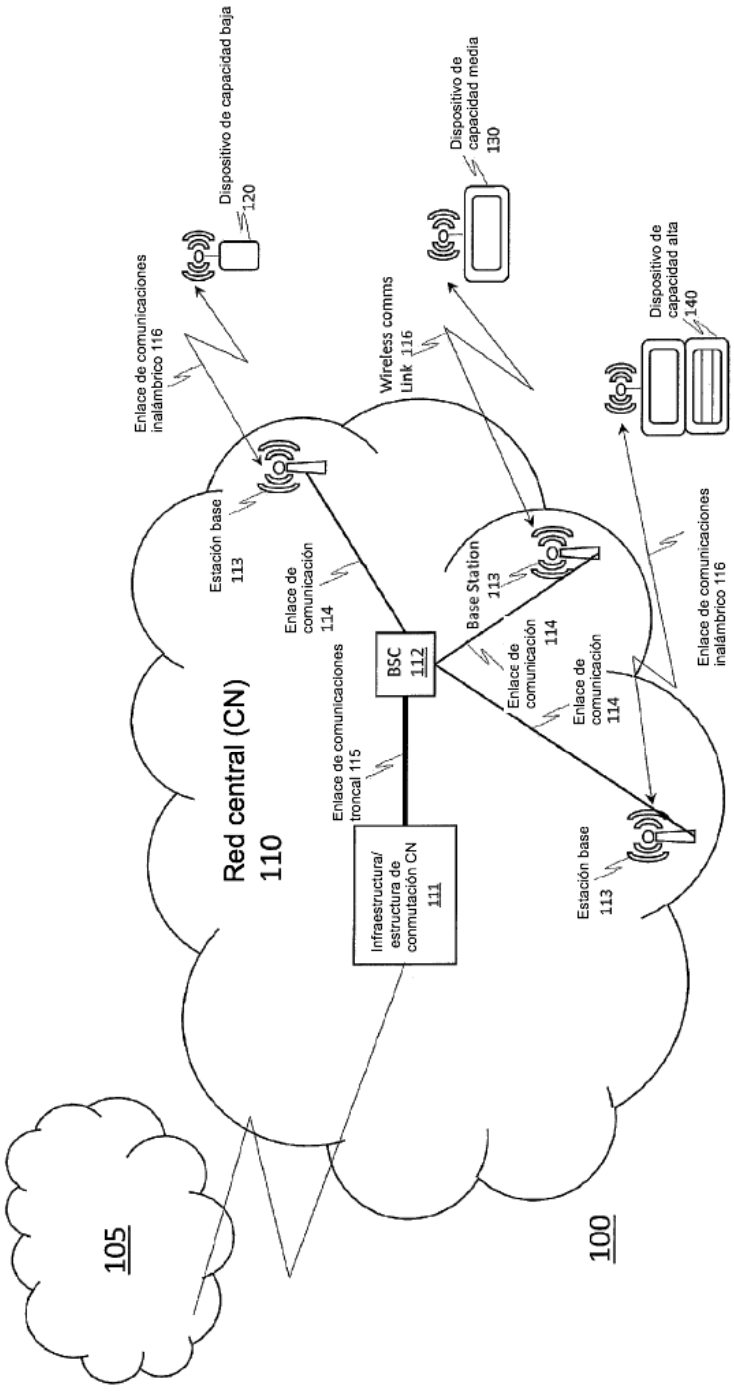
Dispositivo de capacidad baja
120
Dispositivo de capacidad media
130
Dispositivo de capacidad alta
140
Enlace de comunicaciones inalámbrico 116
Wireless comms Link 116
Enlace de comunicaciones inalámbrico 116
Estación base 113
Enlace de comunicación 114
Base Station 113
Enlace de comunicación 114
Enlace de comunicación 114
Enlace de comunicaciones troncal 115
BSC 112
Red central (CN) 110
Infraestructura/ estructura de conmutación CN 111
Estación base 113
105
100

Figura 1

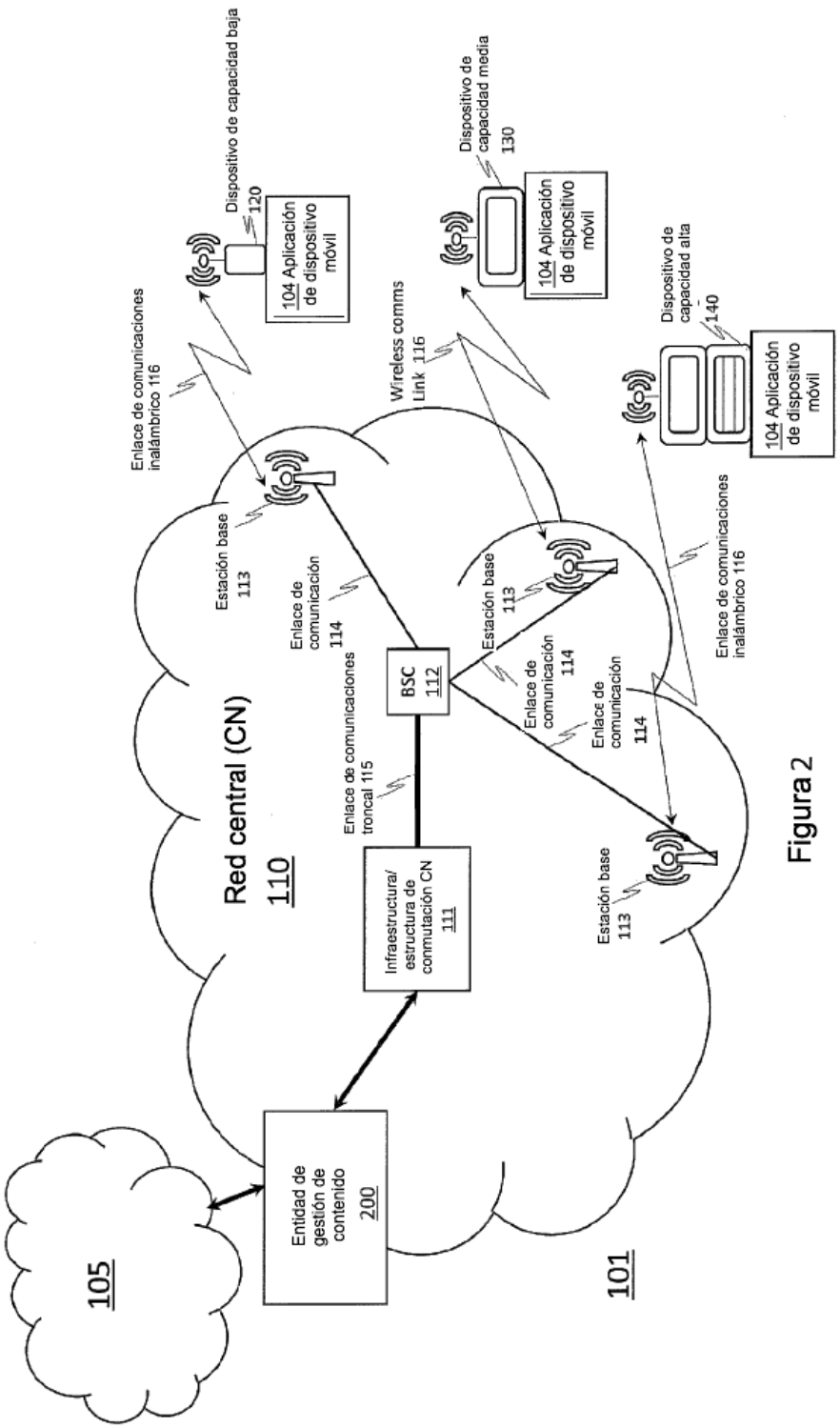
Dispositivo de capacidad baja
120
104 Aplicación de dispositivo móvil
Dispositivo de capacidad media
130
104 Aplicación de dispositivo móvil
Dispositivo de capacidad alta
140
104 Aplicación de dispositivo móvil
Enlace de comunicaciones inalámbrico 116
Wireless comms Link 116
Enlace de comunicaciones inalámbrico 116
Estación base 113
Enlace de comunicación 114
Estación base 113
Enlace de comunicación 114
Enlace de comunicación 114
Estación base 113
BSC 112
Enlace de comunicaciones troncal 115
Red central (CN) 110
Infraestructura/ estructura de conmutación CN 111
Entidad de gestión de contenido 200
105
101

Figura 2

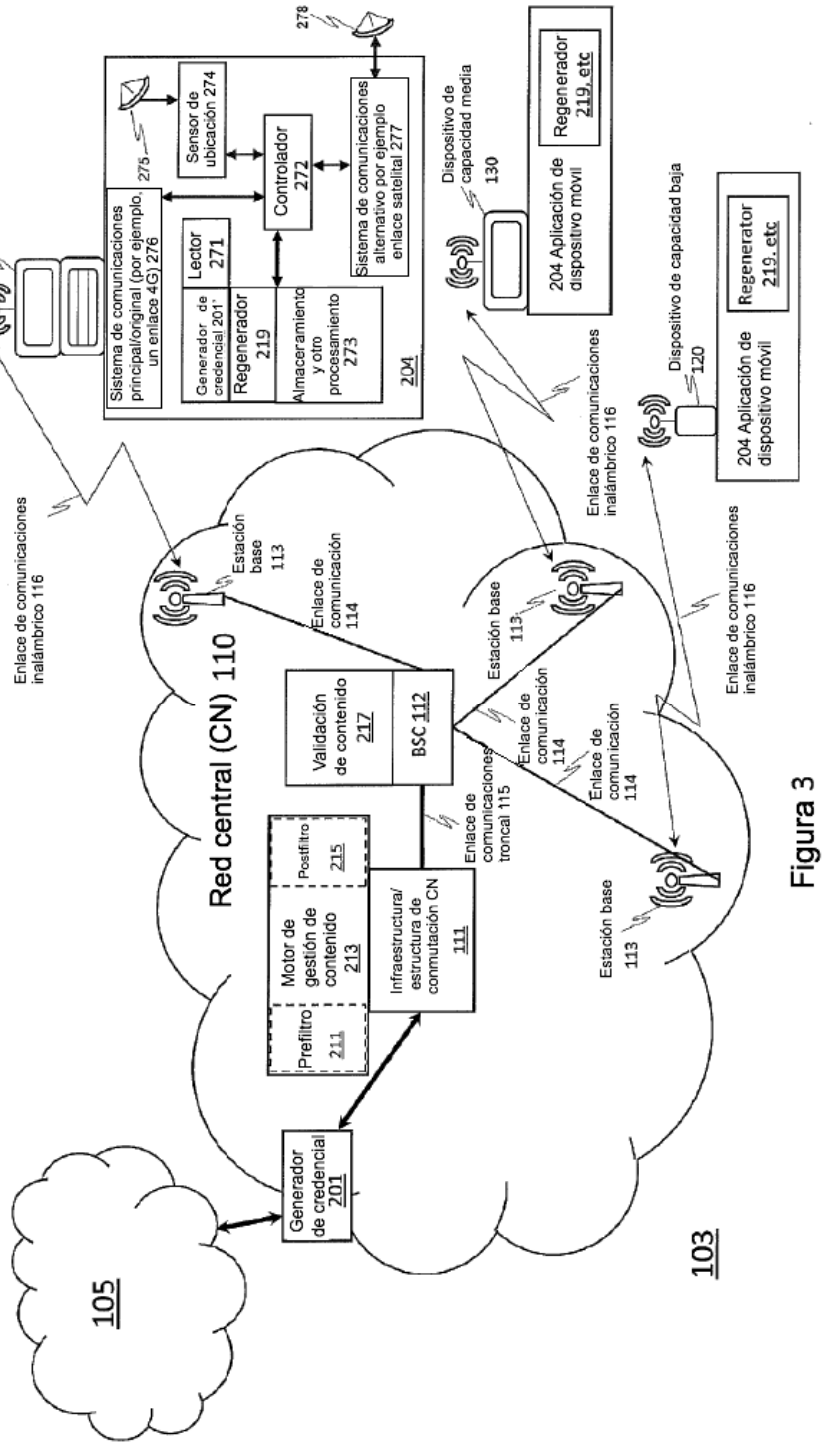
Dispositivo de capacidad alta 140
Sistema de comunicaciones principal/original (por ejemplo, un enlace 4G) 276
Sensor de ubicación 274
Controlador 272
Lector 271
Generador de credencial 201
Regenerador 219
Almacenamiento y otro procesamiento 273
Sistema de comunicaciones alternativo por ejemplo enlace satelital 277
204
275
278
Dispositivo de capacidad media 130
204 Aplicación de dispositivo móvil
Regenerador 219, etc
Dispositivo de capacidad baja 120
204 Aplicación de dispositivo móvil
Regenerator 219, etc
Enlace de comunicaciones inalámbrico 116
Enlace de comunicaciones inalámbrico 116
Enlace de comunicaciones inalámbrico 116
Enlace de comunicaciones inalámbrico 116
Estación base 113
Enlace de comunicación 114
Estación base 113
Enlace de comunicación 114
Enlace de comunicación 114
Estación base 113
Red central (CN) 110
Validación de contenido 217
BSC 112
Enlace de comunicaciones troncal 115
Infraestructura/ estructura de conmutación CN 111
Motor de gestión de contenido 213
Postfiltro 215
Prefiltro 211
Generador de credencial 201
105
103

Figura 3

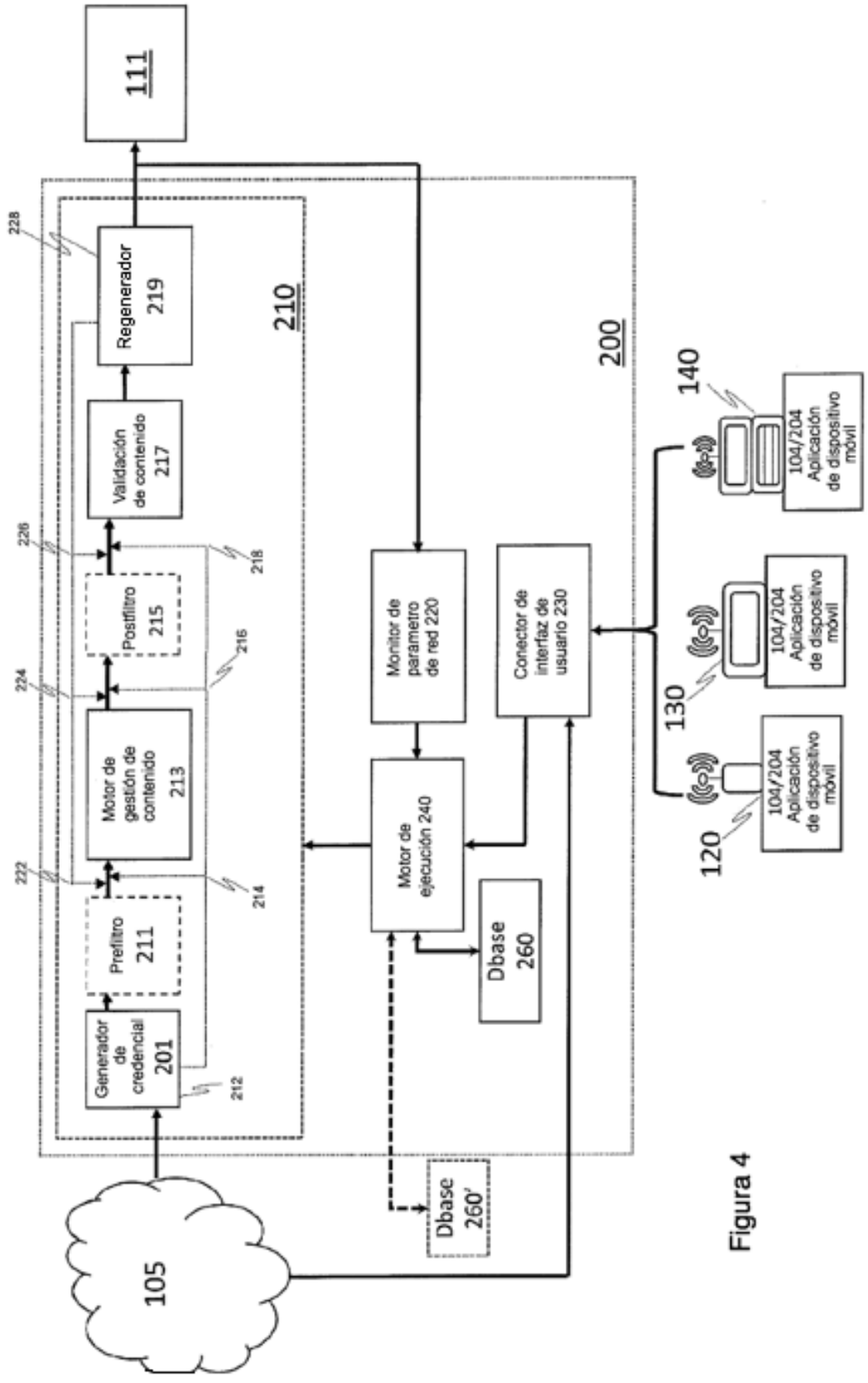
111
210
200
228
Regenerador 219
Validación de contenido 217
226
218
Postfiltro 215
216
224
Motor de gestión de contenido 213
222
214
Prefiltro 211
Generador de credencial 201
212
Monitor de parametro de red 220
Conector de interfaz de usuario 230
Motor de ejecución 240
Dbase 260
Dbase 260'
105
140
104/204 Aplicación de dispositivo móvil
130
104/204 Aplicación de dispositivo móvil
120
104/204 Aplicación de dispositivo móvil

Figura 4

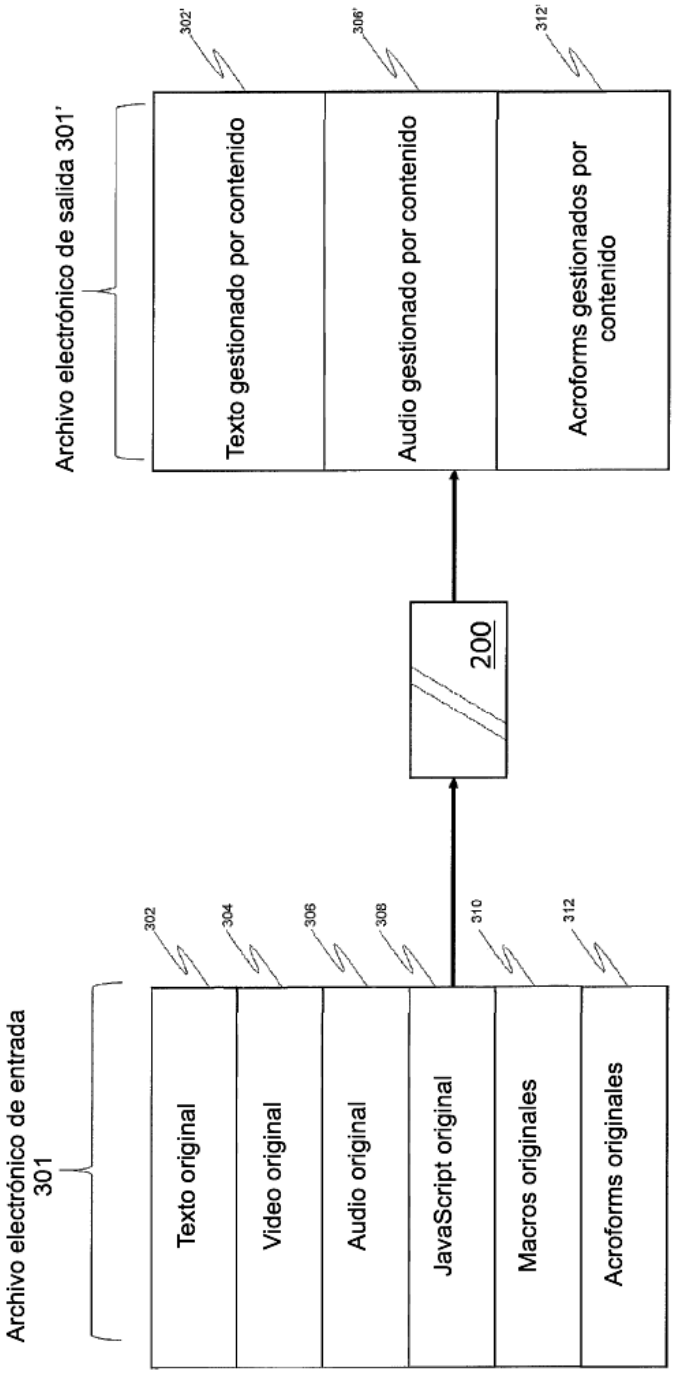
Archivo electrónico de entrada
301
Texto original
Video original
Audio original
JavaScript original
Macros originales
Acroforms originales
302
304
306
308
310
312
200
Archivo electrónico de salida 301'
Texto gestionado por contenido
Audio gestionado por contenido
Acroforms gestionados por contenido
302'
306'
312'

Figura 5

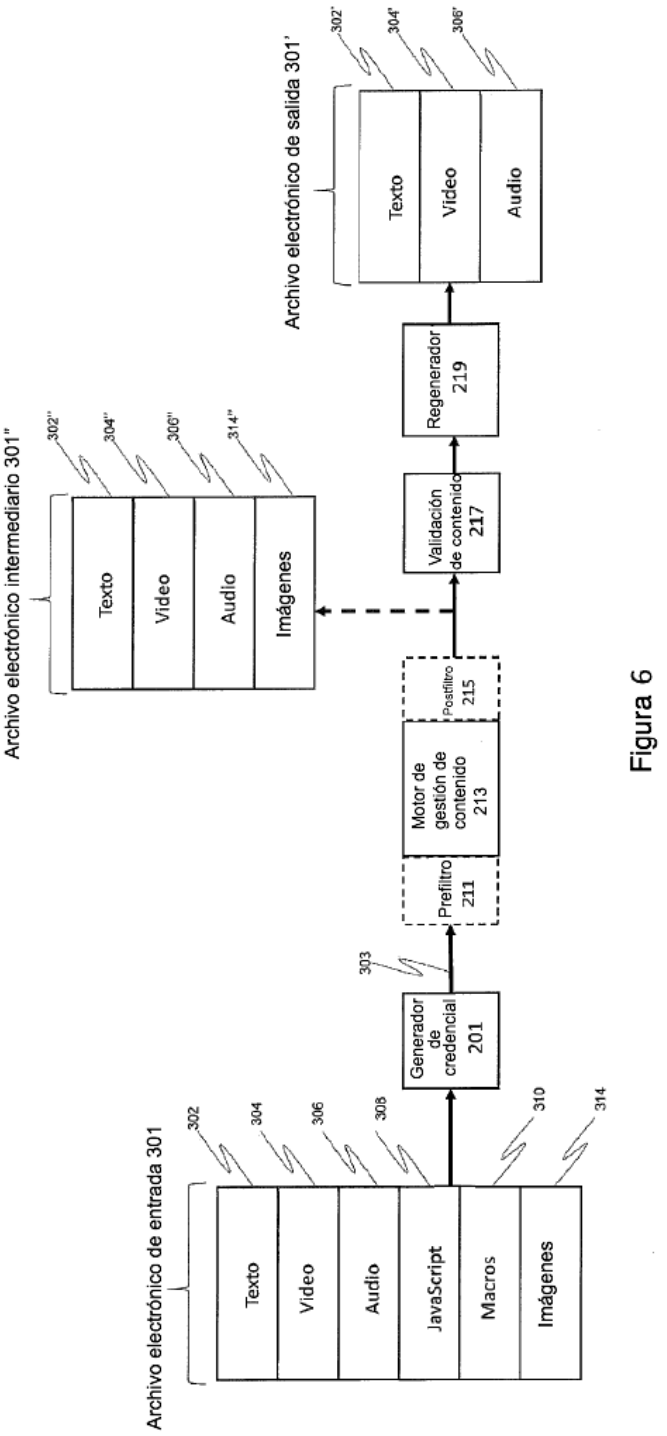
Archivo electrónico de entrada 301
Texto
Video
Audio
JavaScript
Macros
Imágenes
302
304
306
308
310
314
303
Generador de credencial 201
Prefiltro 211
Motor de gestión de contenido 213
Postfiltro 215
Validación de contenido 217
Regenerador 219
Archivo electrónico intermediario 301"
Texto
Video
Audio
Imágenes
302"
304"
306"
314"
Archivo electrónico de salida 301'
Texto
Video
Audio
302'
304'
306'

Figura 6

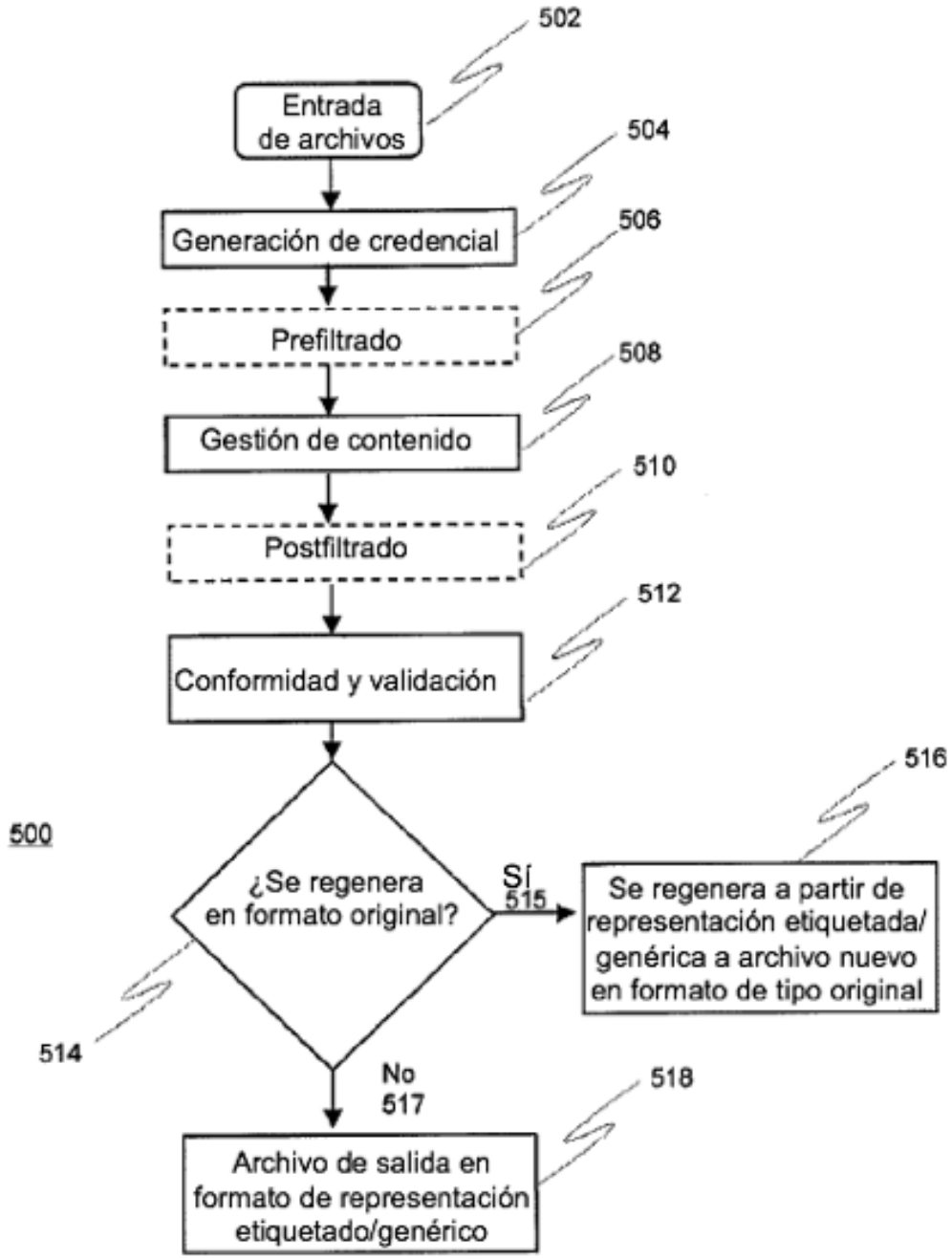
502
Entrada de archivos
504
Generación de credencial
506
Prefiltrado
508
Gestión de contenido
510
Postfiltrado
512
Conformidad y validación
500
¿Se regenera en formato original?
514
Sí
515
516
Se regenera a partir de representación etiquetada/ genérica a archivo nuevo en formato de tipo original
No
517
518
Archivo de salida en formato de representación etiquetado/genérico

Figura 7


Archivo electrónico de entrada 301
TIPO DE ARCHIVO DE ENTRADA (ARCHIVO ORIGINAL)
506
PREFILTRO (CICLO 0) – OPCIONAL
CARGA ALMACENAMIENTO DE ENTRADA DESDE EL ARCHIVO
GENERA CREDENCIALES EN UN ALMACENAMIENTO DE CONTEXTO
APLICA PREFILTRO A CREDENCIALES
CREA ALMACENAMIENTO REGENERADO DE CREDENCIALES
ALMACENAMIENTO DE MEMORIA DE ENTRADA
ALMACENAMIENTO DE MEMORIA DE CONTEXTO
ALMACENAMIENTO DE MEMORIA INTERMEDIA
ALMACENAMIENTO DE MEMORIA DE SALIDA
702
704
706
708
508
GESTIÓN/LIMPIEZA DE CONTENIDO (CICLO 1)
INTERCAMBIO DE ALMACENAMIENTO DE ENTRADA y SALIDA
GENERA CREDENCIALES EN UN ALMACENAMIENTO DE CONTEXTO
APLICA GESTIÓN DE CONTENIDO A CREDENCIALES
APLICA CORRECCIONES SEMÁNTICAS A CREDENCIALES
CREA ALMACENAMIENTO REGENERADO DE CREDENCIALES
ALMACENAMIENTO DE MEMORIA DE ENTRADA
ALMACENAMIENTO DE MEMORIA DE CONTEXTO
ALMACENAMIENTO DE MEMORIA INTERMEDIA
ALMACENAMIENTO DE MEMORIA DE SALIDA
710
712
714
716
510
POSTFILTRO (CICLO 2) – OPCIONAL
INTERCAMBIO DE ALMACENAMIENTO DE ENTRADA Y SALIDA
GENERA CREDENCIALES EN UN ALMACENAMIENTO DE CONTEXTO
APLICA POSTFILTRO A CREDENCIALES
CREA ALMACENAMIENTO REGENERADA DE CREDENCIALES
ALMACENAMIENTO DE MEMORIA DE ENTRADA
ALMACENAMIENTO DE MEMORIA DE CONTEXTO
ALMACENAMIENTO DE MEMORIA INTERMEDIA
ALMACENAMIENTO DE MEMORIA DE SALIDA
718
720
722
724
512
VALIDACIÓN (CICLO 3)
INTERCAMBIO DE ALMACENAMIENTO DE ENTRADA Y SALIDA
GENERA CREDENCIALES EN UN ALMACENAMIENTO DE CONTEXTO
VALIDA/PROTEGE VERIFICACIÓN DE TOKEN
CREA ALMACENAMIENTO REGENERADO DE CREDENCIALES
ALMACENAMIENTO DE MEMORIA DE ENTRADA
ALMACENAMIENTO DE MEMORIA DE CONTEXTO
ALMACENAMIENTO DE MEMORIA INTERMEDIA
ALMACENAMIENTO DE MEMORIA DE SALIDA
726
728
730
732
TIPO DE ARCHIVO DE SALIDA (archivo regenerado)

Figura 8