# Control de Acceso en Redes Sociales Web

Lorena González-Manzano
Univ. Carlos III de Madrid
Leganés, España
lgmanzan@inf.uc3m.es

Ana I. González-Tablas
Univ. Carlos III de Madrid
Leganés, España
aigonzal@inf.uc3m.es

José M. de Fuentes
Univ. Carlos III de Madrid
Leganés, España
jfuentes@inf.uc3m.es

Benjamín Ramos Álvarez
Univ. Carlos III de Madrid
Leganés, España
benja1@inf.uc3m.es

***Resumen*—Recientemente, motivados por la expansión de internet y la aparición de las Redes Sociales Web (RSW), han surgido gran cantidad de problemas y retos asociados con la privacidad. Uno de los problemas principales es el diseño y la implementación de sistemas que posibiliten a los usuarios la gestión del control de acceso. A este respecto, pero en el contexto de las RSW, se han identificado una serie de requisitos. Sin embargo, en la literatura, los trabajos existentes sólo satisfacen parcial o completamente algunos de ellos. En este artículo, se propone primero un modelo de control de acceso, $SoNeUCON_{ABC}$, el cual extiende el modelo $UCON_{ABC}$, junto con la especificación de un mecanismo que lo implementa. En segundo lugar, se proporcionan directrices para el establecimiento de mecanismos que, desplegados sobre $SoNeUCON_{ABC}$, satisfagan todos los requisitos.**

***Palabras Clave*—Control de acceso centrado en usuarios, Redes sociales web, Interoperabilidad, *Sticky-policies*, Minimización de datos expuestos.**

## I. Introducción

Internet se ha convertido en el principal medio de comunicación, produciéndose un incremento tanto en la cantidad de usuarios como en los servicios disponibles. De hecho, las Redes Sociales Web (RSW) son uno de los medios de comunicación más recientes. Desde el comienzo de las redes sociales en 1997, hasta su establecimiento con Friendster en 2002, muchas han aparecido y su uso se ha intensificado [16].

Por el contrario, a pesar del incremento de los usuarios de las RSW, muchas características no se consideran, como es la privacidad, la cual se define como "La condición de no tener conocimiento sobre algo poseído por otra persona"[4]. Las RSW son sistemas que almacenan cientos de datos personales, los cuales deben ser cuidadosamente protegidos. Sin embargo, este hecho no es apreciado por los usuarios. Por ejemplo, J. Becker *et al.* realizaron un estudio en el que se mostraba que ningún usuario de Facebook (según la muestra analizada) había utilizado los mecanismos de seguridad proporcionados [11]. Igualmente, Acquisti *et al.* estudiaron que incluso los usuarios de Facebook que son conscientes de los problemas de privacidad, continúan usándola [2].

Independientemente de los intereses de los usuarios, la privacidad es una pieza clave de nuestra vida tal y como subrayan las leyes y los derechos. Por ejemplo, en la Declaración Universal de los Derechos Humanos se establece el derecho a que nadie ha de ser objeto de injerencias arbitrarias en su vida privada, familiar o correspondencia [1].

Considerando la importancia de la privacidad junto con el éxito de las RSW, una gran pregunta se plantea: ¿las RSW proporcionan los mecanismos necesarios para preservar la privacidad? La respuesta está lejos de ser trivial, e incluso una pregunta previa tampoco dispone de una respuesta clara y concisa: ¿cuáles son los requisitos para proteger la privacidad de los usuarios en las RSW? En 2007, Gates identificó un conjunto de requisitos para permitir que los usuarios gestionasen sus recursos en las RSW [6]. Estos requisitos establecen que los sistemas de control de acceso de las RSW deben estar *basados en relaciones*, proporcionar *grano fino*, posibilitar la *interoperabilidad* y seguir el paradigma denominado *sticky-policy*. Desde entonces muchos trabajos de investigación han propuesto sistemas de control de acceso que satisfacen, total o parcialmente, algunos de los requisitos. Sin embargo, no existe ningún camino concreto que guíe a los investigadores y a la industria en la tarea de desarrollar sistemas de control de acceso para RSW que incluyan todos los requisitos.

En este trabajo, los requisitos de Gates se toman como punto de partida y, atendiendo a las tendencias actuales, se añade la *minimización de datos expuestos*.

La contribución principal de este trabajo es la creación de un modelo de control de acceso, denominado $SoNeUCON_{ABC}$, capaz de satisfacer (desde un punto de vista teórico) los cinco requisitos, así como el mecanismo que lo implementa, el cual únicamente satisface (desde un punto de vista práctico) los requisitos de *basados en relaciones* y *grano fino*. El modelo es una extensión del modelo de control de uso $UCON_{ABC}$ [20]. En segundo lugar, se establecen directrices para el desarrollo de mecanismos que, desplegados sobre $SoNeUCON_{ABC}$, satisfacen cada uno de los requisitos identificados.

El resto del artículo se estructura del siguiente modo. En la Sección II se describen brevemente modelos y mecanismos de control de acceso existentes. En la Sección III se detallan los requisitos identificados por Gates [6], añadiendo uno nuevo. Posteriormente, en la Sección IV se expone la conceptualización de una RSW. En la Sección V se especifica el modelo de control de acceso propuesto, $SoNeUCON_{ABC}$, así como el mecanismo que lo implementa y las directrices necesarias para el desarrollo de mecanismos que satisfagan los requisitos de *interoperabilidad*, *sticky-policies* y *minimización de datos expuestos*. Finalmente, en la Sección VI se presentan las conclusiones y los retos futuros.

## II. Antecedentes

Actualmente se identifican tres modelos tradicionales de control de acceso: *Mandatory Access Control (MAC)*, en el

que los objetos y los sujetos se clasifican en relación con niveles de seguridad y el acceso se otorga en función de ellos; *Discretionary Access Control (DAC)*, en el que el acceso a la información se efectúa en relación con la identidad de los usuarios y con un conjunto de autorizaciones y reglas; y *Role Based Access Control (RBAC)*, basado en la definición de distintos roles a los que se les asignan permisos y, posteriormente, los roles son asignados a los distintos sujetos [19].

Además de los anteriores, se han desarrollado modelos como *Relationship Based Access Control* (RelBAC) [3], en el que los permisos son modelados como relaciones entre los usuarios y los datos, o *Attribute Based Access Control (ABAC)* [24], enfocado en la definición de políticas considerando atributos de los sujetos, los recursos y el entorno. Bajo la perspectiva de ABAC se ha creado *Usage Control Model* ($UCON_{ABC}$) ([20], [10]). Se basa en la presentación de un marco uniforme para el control de acceso, en el que se pueden combinar los sistemas MAC, DAC, RBAC e incluso DRM (Gestión Digital de Derechos, *Digital Rights Management*).

Más detalladamente, el modelo $UCON_{ABC}$ considera ocho componentes: *sujetos (S)*, que son entidades que ejercen derechos sobre objetos; *objetos (O)*, que son entidades sobre las que los sujetos tienen derechos; *atributos de sujetos (AT(S))* y *atributos de objetos (AT(O))* que se refieren a características asociadas con los sujetos y con los objetos respectivamente; *deRechos (R)*, los cuales se reconocen como privilegios ejercidos sobre objetos tales como la lectura o la escritura; *Autorizaciones (A)*, que se corresponden con predicados que contienen AT(S) y AT(O) que se evalúan para decidir si un derecho solicitado por un sujeto sobre un objeto concreto debe otorgarse o denegarse; *oBligaciones (B)*, que representan predicados que se deben satisfacer antes, durante y después de que un derecho sea concedido; y *Condiciones (C)*, que se corresponden con factores del entorno o del sistema no controlados por los sujetos.

## III. Requisitos para otorgar control de acceso en RSW

En [6] se identifican un conjunto de requisitos esenciales para desarrollar exitosamente la gestión de control de acceso en la Web 2.0, incluyéndose las RSW. Estos requisitos son:

1. *Basados en relaciones*: los administradores de los datos (ej., dueños de los datos) controlan la entrega de datos mediante relaciones establecidas con los solicitantes de los mismos, en lugar de realizar las entregas en base al rol o a cualquier otra característica de dichos solicitantes.
2. *Grano fino*: los usuarios deben controlar su información escogiendo con el mayor grano fino posible quién puede acceder a ella y bajo qué circunstancias. Debe ser posible escoger políticas de grano fino considerando tanto a los datos como a los solicitantes.
3. *Interoperabilidad*: los usuarios acceden a múltiples RSW y quieren que sus datos sean tratados de forma similar en todas ellas. Los sistemas de control de acceso deberían ser interoperables entre distintas RSW para que las preferencias de los usuarios prevalezcan con independencia de la RSW a la que se acceda. Este problema se conoce como *Walled Garden Problem* [12].
4. *Sticky-policy*: las políticas deben seguir a los datos a los que aplican, previniendo revelaciones no autorizadas con posterioridad a la entrega de datos. Es importante considerar que amenazas externas como grabaciones de datos no son contempladas.

En este trabajo se identifica un quinto requisito, *minimización de datos expuestos*, contra los servicios de almacenamiento honestos-pero-curiosos. Los servidores han de proteger la información almacenada contra posibles amenazas, pero los usuarios desconocen las técnicas y los procedimientos con los que se realiza dicha protección. De hecho, la información personal es completamente susceptible a ser utilizada por compañías, especialmente las de publicidad, para mejorar y desarrollar productos acordes a las preferencias de los usuarios. Por tanto, es deseable que los usuarios controlen su información personal sin permitir el acceso no autorizado a los servidores en los que se almacena.

## IV. Conceptualización de una RSW

En esta Sección se presenta la conceptualización de una RSW para establecer las bases de la propuesta.

### *IV-A. Datos*

En una RSW el conjunto de datos que se consideran es muy diverso. Se incluyen fotos, vídeos, mensajes en el muro y mensajes personales que son privados y dirigidos a un usuario concreto o a un grupo. El conjunto de todo tipo de datos será denominado *D*.

Adicionalmente, los datos tienen un conjunto de atributos asociados, cuya representación es $dAT = \{dat_1, dat_2, ..., dat_{n_{dAT}}\}$. Los atributos de los datos pueden clasificarse en dos grupos. El primero involucra características propias de los datos como el tipo, la fecha o la hora de creación. El segundo grupo se refiere a cualquier característica que puede ser asignada a los datos, por ejemplo el hecho de ser privado, confidencial, público, etc.

### *IV-B. Acciones*

En una RSW se pueden realizar acciones sobre los datos, denotadas *ACC*. Principalmente se pueden identificar cuatro acciones: *lectura*, equivalente a la visualización de cualquier tipo de contenido; *modificación*, equivalente a la escritura de etiquetas en vídeos o fotos, o a la modificación de comentarios previamente escritos; *inserción*, equivalente a la subida de una foto o de un vídeo a una RSW; y *borrado*.

### *IV-C. Usuarios*

El conjunto de usuarios de una RSW se identifica como *V*. A grandes rasgos, los usuarios pueden clasificarse en solicitantes, aquellos que solicitan un determinado derecho sobre un dato, y administradores, aquellos que administran el acceso a los datos. Por tanto, se deja para trabajo futuro el problema de la co-propiedad, siendo un ejemplo de ello "si un usuario A hace una foto de un usuario B y la sube al espacio de otro usuario C en una RSW, ¿quién es propietario de la foto?".

Al igual que los datos, los usuarios también tienen asociados un conjunto de atributos, correspondientes con $vAT = \{vat_1, vat_2, ..., vat_{n_{vAT}}\}$. Por un lado, un perfil de un usuario se asocia con una nacionalidad, edad, estilo musical, etc. Por otra parte, hay otro conjunto de atributos, denominados atributos de contexto, que describen el estado emocional del usuario o la actividad que está desarrollando.

### *IV-D. Relaciones*

En una RSW un usuario puede aceptar o rechazar el establecimiento de una relación con otro usuario de la RSW. Teniendo en cuenta que las relaciones entre usuarios son una de las características principales de estos sistemas, comúnmente estos sistemas son identificados como un grafo. Un grafo se caracteriza por tener una gran cantidad de entidades, denominadas nodos, y de conexiones entre nodos, llamadas aristas. En términos generales, cuando se modela una RSW como un grafo, los usuarios se corresponden con los nodos y las relaciones con las aristas. Este tipo de representación ha sido utilizada recientemente por muchos autores ([9], [8], [7]). Además, se considera que entre dos usuarios de una RSW puede existir una relación directa o indirecta.

Las relaciones directas entre dos usuarios se identifican como *E* y están asociadas con un conjunto de atributos, denotados como $eAT = \{eat_1, eat_2, ..., eat_{n_{eAT}}\}$. Los atributos más importantes son la dirección y el tipo de las relaciones. Por el contrario, un par de usuarios pueden estar relacionados indirectamente, existiendo un camino ordenado de aristas o relaciones directas que conecta ambos nodos, el cual se refiere a la longitud de la relación.

Por una parte, en relación con la dirección de las relaciones, éstas pueden ser unidireccionales o bidireccionales [8]. Las primeras se corresponden con las relaciones en las que la solicitud sólo se establece en un único sentido.

Por el contrario, las relaciones bidireccionales requieren que el par de nodos asociados con una solicitud, una vez aceptada, tengan el mismo tipo de relación en ambas direcciones.

Por otra parte, el significado semántico o el rol de una relación implica disponer de distintas relaciones como 'amigo', 'profesional', 'familia', etc. Algunas RSW utilizan un único rol, como en LinkedIn, mientras que otras consideran múltiples roles. Además, dos nodos pueden vincularse por varias relaciones direccionales, cada una con un rol diferente.

Asimismo, las relaciones pueden tener otros atributos como la fecha y la hora de creación, el historial, etc. Adicionalmente, los usuarios pueden vincular múltiples atributos a sus relaciones, como el nivel de confianza (la fuerza o la debilidad de una relación) [8] o la duración (validez de la relación).

### *IV-E. Contexto*

Por último, la información de contexto es otro aspecto a valorar. El conjunto de estas características se identifica con *CX* y se incluyen factores dinámicos y externos, como es el estado de comunicación de la red, la disponibilidad del servicio o parámetros asociados con la calidad.

## V. Propuesta para Facilitar a los Usuarios la Gestión del Control de Acceso en una RSW

Una de las propuestas de este trabajo consiste en explorar soluciones enfocadas al control de acceso que satisfacen los cinco requisitos identificados en la Sección III. Más concretamente, las contribuciones se basan en la definición de un modelo de control de acceso (Sección V-A) y del mecanismo asociado para satisfacer los requisitos de *basados en relaciones* y *grano fino* (Sección V-B), y en la especificación de directrices para el desarrollo de mecanismos que satisfagan los tres requisitos restantes (Sección V-C).

### *V-A. Extendiendo el modelo $UCON_{ABC}$ para considerar relaciones*

En principio, para satisfacer el requisito de *basados en relaciones*, el enfoque indicado por RelBAC (Sección II) puede señalarse como la propuesta ideal para RSW. Sin embargo, aunque una de las principales características de las RSW es que están basadas en relaciones, se necesitan sistemas de control de acceso que sean capaces de considerar políticas de grano fino en relación con los atributos de los datos y de los solicitantes. Por ejemplo, las redes sociales basadas en la localización consideran la posición, la cual es una característica relacionada con los usuarios y difícil de gestionar por medio de relaciones.

Por otra parte, los sistemas de control de acceso que siguen el enfoque ABAC consideran los atributos de los usuarios, de los datos y (no siempre) del contexto, como elementos principales en las políticas de control de acceso, los cuales son analizados al decidir si una acción solicitada es autorizada o no. Este enfoque permite establecer control de acceso de grano fino. En este trabajo el modelo $UCON_{ABC}$ se escoge como el modelo ABAC por ser el modelo de este tipo más representativo y maduro [20].

Asumiendo el uso del modelo $UCON_{ABC}$, las relaciones se pueden incluir de múltiples modos en el proceso de decisión de una autorización. Primero, las relaciones pueden definirse como un atributo de la entidad origen de una relación, ej. un usuario, Alice, tiene una lista de 'amigos', una lista de 'conocidos', una lista de 'trabajadores', etc., siendo estas listas sus atributos. Éste es el enfoque de algunas de las recientes propuestas construidas sobre $UCON_{ABC}$ ([21], [5]). Incluso el modelo administrativo descentralizado de Salim *et al.*, el cual puede ser aplicado directamente en las RSW, toma este enfoque [14]. No obstante, esta perspectiva no es suficiente en las RSW porque resulta compleja la consideración de los atributos de las relaciones directas e indirectas. Según discute Fong en [13], en algunos contextos es más natural modelar relaciones como elementos binarios relacionados, en lugar de predicados unitarios. Por ejemplo, considerando $UCON_{ABC}$ y el modelo administrativo de Salim *et al.* ([14], [22]), la relación " Alice es amiga de Bob con un nivel de confianza 3 y Bob es amigo de Alice con un nivel de confianza 3" puede ser ligeramente modelado como " Alice dice Bob es amigo si confianza[3]". Sin embargo, en situaciones como ésta, correspondiente con una relación bidireccional y con

atributos con valores concretos, los predicados asociados pueden requerir bastante complejidad. Por este motivo, en este trabajo se considera más apropiado modelar las relaciones como relaciones binarias.

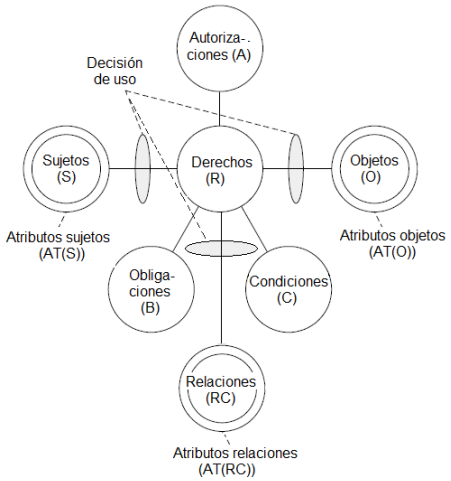


Figura 1. $SoNeUCON_{ABC}$

El modelo presentado, $SoNeUCON_{ABC}$, extiende el modelo $UCON_{ABC}$ y establece una nueva entidad, *relación* ($RC$), y un conjunto de atributos de dicha entidad, *atributos de relación* ($AT(RC)$), Figura 1. El conjunto de entidades, atributos y funciones originales identificadas en el modelo $UCON_{ABC}$ también se consideran en este nuevo modelo. Además, los elementos de la conceptualización pueden asociarse con algunos de los pertenecientes al modelo $SoNeUCON_{ABC}$:

- *Sujetos* ($S$) son los usuarios de las RSW ($V$ en la conceptualización), previamente identificados como administradores o solicitantes; adicionalmente, $AT(S) \subseteq vAT$.
- *Objetos* ($O$) son los datos de las RSW ($D$), identificados como fotos, vídeos, mensajes en los muros y mensajes personales; adicionalmente, $AT(O) \subseteq dAT$.
- *Relaciones* ($RC$) representan el conjunto de relaciones existentes entre un par de usuarios de una RSW, ej. si unos usuarios son $v_i$ y $v_j$, este conjunto es $P_{v_i,v_j}$. Comúnmente, estos dos usuarios son el solicitante y el administrador del objeto del que se está solicitando acceso.
- *Derechos* ($R$) se refieren a las acciones ($ACC$) que pueden ser realizadas en una RSW, como es la lectura, la modificación o el borrado.
- *Autorizaciones* ($A$) son las reglas definidas como predicados funcionales, las cuales han de ser satisfechas para que a un sujeto se le otorgue un derecho sobre un objeto. Estas reglas se conocen con el nombre de políticas.
- *Obligaciones* ($B$) se refieren a las actividades que tienen que ser realizadas por los usuarios antes y mientras el proceso de uso se ejecuta.
- *Condiciones* ($C$) se corresponden con las características del contexto ($CX$) mencionadas anteriormente, tales como la disponibilidad de la red.

A pesar de que la formalización de este modelo es objeto de trabajo futuro, es posible indicar que la gestión del acceso se realiza mediante políticas. Por este motivo, para ofrecer un visión global de cómo realizar dicha gestión, la construcción de las políticas se ilustra posteriormente para el caso del modelo de pre-autorizaciones [1].

*Ejemplo:* En [23], se propone un ejemplo en el que un usuario, Bart ($s_2$), intenta enviar una invitación de amistad a Ned ($s_4$) (ver Figura 2 para observar el grafo que representa la RSW). Homer ($s_1$), que es el padre de Bart y que por ello tiene permisos de administración sobre las acciones de Bart, dispone de una política que dice que 'cualquier persona que sea su co-trabajador o un amigo directo de su co-trabajador, no podrá ser amigo de sus hijos'. Este ejemplo corresponde con las utilidades de un multi-administrador, que se deja como trabajo futuro; sin embargo, se puede mostrar cómo las autorizaciones pueden definirse bajo el modelo propuesto. Las autorizaciones serán evaluadas en relación con el conjunto de relaciones $RC_{s_1,s_i}$, siendo $s_i$ el administrador del objeto $o$ (la invitación de amistad, en el espacio de Ned) y $r$ la acción asociada con escribir el derecho solicitado.

1. $TIPODATO$ es el conjunto de datos considerados en la RSW.
2. $tipodato : O \rightarrow TIPODATO$; es el atributo del dato indicando el tipo del dato (como una invitación para establecer un determinado tipo de relación en la RSW).
3. $ROL$ es el conjunto de roles que pueden ser asociados con una relación directa.
4. $rol\,[i] : RC \rightarrow ROL$; es un atributo de $RC$ que refleja el rol de la i-ésima relación directa del camino considerado.
5. $long : RC \rightarrow \mathbb{N}^+$; es la longitud de la relación, ej., el número $n$ de aristas que la componen.
6. $AT(RC) : \{rol\,[i]\,, long\}$
7. $permitir(s, o, rc, r) \Rightarrow$
   $(\ NOT\ (\ Pred_1\ OR\ Pred_4\ )\ AND\ Pred_5)$
   a) $Pred_1 = (rol\,[0]\,(rt_{s_1,s_i}) = cotrabajador)$
      AND (long($rt_{s_1,s_i}$) $= 1$)
   b) $Pred_2 = (rol\,[0]\,(rt_{s_1,s_i}) = cotrabajador)$
      AND (rol[1] $(rt_{s_1,s_i}) = amigo$)
   c) $Pred_3 = (long(rt_{s_1,s_i}) = 2)$
   d) $Pred_4 = (Pred_2\ AND\ Pred_3)$
   e) $Pred_5 = (tipodato(o) = invitacion(amigo))$

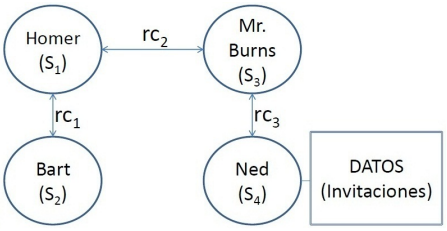


Figura 2. Grafo de la RSW considerada en el ejemplo

### V-B. Mecanismo de control de acceso en $SoNeUCON_{ABC}$

Aunque todos los requisitos pueden ser satisfechos por el modelo, el mecanismo que lo implementa sólo permite satisfacer los requisitos *basados en relaciones* y *grano fino*.

[1] En el modelo de pre-autorizaciones de $UCON_{ABC}$ el proceso de decisión se realiza antes de que el derecho solicitado sea ejecutado, sin considerarse actualizaciones de atributos mientras se ejerce el derecho. En este caso las pre-autorizaciones se denotan como $preA$.

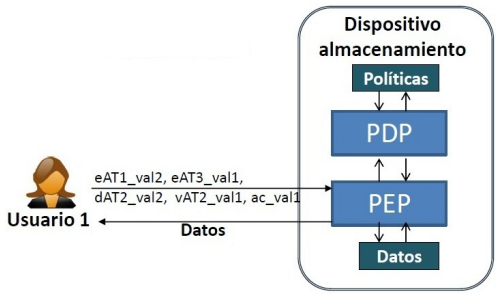


Figura 3. Mecanismo de control de acceso en $SoNeUCON_{ABC}$

Hay múltiples posibilidades de implementarlo. En el enfoque presentado en este documento se propone una arquitectura del lado del servidor en la que se considera un único dominio. Esta propuesta se muestra en la Figura 3, en ella tanto los datos como las políticas se localizan en un único dominio correspondiente con una RSW. Por ello, la RSW asume el rol de PEP (Punto de Aplicación de Políticas, *Policy Enforcement Point*) y de PDP (Punto de Decisión de Políticas, *Policy Decision Point*) del monitor de referencia asociado. Los administradores de los datos o del sistema establecen las políticas de uso o administrativas y, en relación con ellas, la RSW entrega o deniega los datos solicitados.

Las políticas pueden ser definidas según todos los elementos del modelo $SoNeUCON_{ABC}$, pero en este trabajo la discusión se enfoca en los elementos de autorización dado que cuestiones relacionadas con los elementos de las obligaciones o las condiciones no presentan gran diferencia con respecto al modelo $UCON_{ABC}$ y sus implementaciones. Atendiendo a lo comentado, las políticas se pueden desarrollar utilizando atributos de usuarios, relaciones y datos, así como acciones.

En cuanto a la administración del uso de los datos, esta arquitectura necesita que los administradores establezcan las políticas en el dispositivo de almacenamiento (la RSW), vinculadas a los datos. Entonces, si se produce la modificación de una política, lo cual se relaciona con la revocación, ellos únicamente actualizan las políticas y los cambios se hacen efectivos en posteriores solicitudes de acceso. Asimismo, aunque existen diferencias, esta cuestión se relaciona con la continuidad de las funciones de decisión que pueden ser utilizadas si se tienen en cuenta atributos mutables de $UCON_{ABC}$.

Un punto clave es la simplicidad de este mecanismo, tanto para administradores como para los usuarios. Los administradores únicamente crean, establecen y modifican las políticas asociadas a los datos y los usuarios. En cambio, los solicitantes solo envían peticiones al PEP. No obstante, se identifican un par de inconvenientes. Primero, dado que el requisito de *minimización de datos expuestos* no se considera en este mecanismo, los datos no se almacenan bajo el control del usuario y pueden ser comprometidos. Por tanto, se ha de depositar la confianza en el dispositivo de almacenamiento. Segundo, cada vez que un usuario desee acceder a un determinado dato, las políticas han de ser satisfechas. De este modo, la aplicación de las políticas se realiza con alta frecuencia, pudiéndose producir un cuello de botella en el dispositivo de almacenamiento (rendimiento/cantidad de trabajo).

### *V-C. Directrices para satisfacer todos los requisitos*

Atendiendo al mecanismo presentado, éste únicamente satisface dos de los cinco requisitos identificados, *basado en relaciones* y *grano fino*. Por este motivo, posteriormente se indican una serie de directrices para la creación de mecanismos que satisfagan cada uno de los requisitos restantes:

1. *Hacia la interoperabilidad*: la satisfacción de este requisito puede conseguirse mediante el establecimiento, en distintos dominios, de la gestión de las políticas y de los datos. Los administradores establecen las políticas en un servicio de control de acceso concreto, mientras que los datos son almacenados en la RSW. La división entre ambos dominios debería permitir que el servicio de control y el de almacenamiento fueran independientes. Sin embargo, se ha de disponer de un mecanismo de identificación común para poder reconocer las políticas que están asociadas a los datos. Igualmente, dicha distinción ha de posibilitar que las mismas políticas puedan ser utilizadas sobre datos localizados en distintas RSW. Un ejemplo de aplicación se presenta en la propuesta académica PrPl [15], en la que los datos se almacenan en servidores web y el acceso se gestiona por medio de tickets. Otro ejemplo, fuera del mundo académico es la RSW Diaspora [2], cuyo principal objetivo es ofrecer una red social libre y descentralizada.
2. *Hacia sticky-policies*: este requisito puede satisfacerse de distintos modos. En primer lugar, aunque en la práctica carece de utilidad debido al coste requerido, una posible solución es la verificación constante de las políticas permitiendo o denegando determinados derechos. En segundo lugar, para garantizar la protección de los datos se propone el establecimiento de un monitor de referencia en el cliente, el cual actúe atendiendo las indicaciones del monitor de referencia establecido en el servidor (la RSW). Es destacable el hecho de ser un mecanismo únicamente estudiado en entornos académicos, siendo EASiER un ejemplo de ello [18]. Esta propuesta se basa en la inclusión de las políticas en claves o en textos cifrados aplicando critografía basada en atributos.
3. *Hacia la minimización de datos expuestos*: el último de los requisitos puede satisfacerse mediante la aplicación de técnicas criptográficas. Los datos son cifrados y almacenados en la RSW y únicamente los usuarios que dispongan de las claves de descifrado pueden acceder a ellos. Asimismo, hay que tener en cuenta que existen multitud de opciones para efectuar la distribución de dichas claves, como puede ser mediante un servicio de distribución de claves o el envío directo de claves entre usuarios. Un ejemplo asociado a este mecanismo es FlybyNight, una propuesta en la que la información se almacena y se visualiza cifrada en la RSW [17]. Por otro lado, en el entorno no académico se ha desarrollado

[2]http://diasporaproject.org/

Unthink [3] (RSW en fase de pruebas), enfocada en ofrecer a los usuarios control sobre sus datos.

## VI. Conclusiones y Retos Futuros

Uno de los principales problemas que actualmente está atrayendo mayor atención en las RSW es el diseño y la implementación de sistemas que ofrecen a los usuarios la posibilidad de gestionar el control de acceso, tal y como se indica en [6]. Este trabajo contribuye en esta dirección partiendo de los requisitos identificados por Gates y uno añadido. Se propone un modelo de control de acceso, $SoNeUCON_{ABC}$, junto con el mecanismo que lo implementa. Además, se exponen un conjunto de directrices para el desarrollo de mecanismos que satisfagan todos los requisitos.

Mencionado anteriormente (Sección V-A), el siguiente paso se dirige hacia la formalización de $SoNeUCON_{ABC}$, detallando los elementos participantes, las funciones de cada uno de ellos y el modo de realizar la gestión del control de acceso.

Tal y como recientemente identificaban J. Park *et al.* ([23], [21]), una cuestión relevante es la distinción entre usuarios y sesiones, definiendo las políticas en función de la sesión de cada usuario. Por tanto, los trabajos futuros se enfocan en el estudio de nuevas propuestas asociadas con esta cuestión, así como su integración en el modelo propuesto.

Finalmente, otro tema importante en las RSW se asocia con la compleja definición de los derechos que los usuarios y los administradores poseen sobre los datos, relacionado con la co-propiedad. Aunque por simplicidad en este artículo los administradores se reconocen como cualquier usuario que es propietario de un objeto o realiza tareas administrativas sobre el mismo, ambos tipos han de distinguirse.

## Referencias


[1] Naciones unidas. http://www.un.org/es/documents/udhr/.

[2] Craig Calhoun. Imagined communities y indirect relationships: Large scale social integration y the transformation of everyday life. 1991.

[3] P. W. L. Fong. Relationship−based access control: protection model and policy language. In *Proc. of the first ACM conf. on Data and app. security and privacy*, CODASPY '11, pages 191–202. ACM, 2011.

[4] W. A. Parent. Privacy, morality, and the law. *Philosophy y Public Affairs*, 12(4):269–288, 1983.

[5] R. Park, J. y Sandhu. ACON: Activity−Centric Access Control for Social Computing. 2011.

[6] E. Gates y Dr. Carrie. Access control requirements for web 2.0 security and privacy. In *Proc. of Wks. on Web 2.0 Security & Privacy (W2SP 2007)*, 2007.

[7] B. Carminati y E. Ferrari. Privacy−aware collaborative access control in web−based social networks. In *Proc. of the 22nd annual IFIP WG 11.3 working conf. on Data and App. Security*, pages 81–96. Springer−Verlag, 2008.

[8] B. Carminati y E. Ferrari y A. Perego. Rule−Based Access Control for Social Networks. In *Proc. OTM 2006 Wks. (On the Move to Meaningful Internet Systems)*, volume 4278 of *LNCS*, pages 1734–1744. Springer, 2006.

[9] B. Carminati y E. Ferrari y A. Perego. Private relationships in social networks. In *Proc. of the 2007 IEEE 23rd Intl. Conf. on Data Engineering Wks.*, pages 163–171. IEEE Computer Society, 2007.

[10] A. Lazouski y F. Martinelli y P. Mori. Usage control in computer security: A survey. *Computer Science Review*, 4(2):81–99, 2010.

[11] J. Becker y H. Chen. Measuring Privacy Risk in Online Social Networks. In *Proc. of W2SP 2009: Web 2.0 Security y Privacy*, 2009.

[12] C. Yeung y I. Liccardi y L. Kanghao y O. Seneviratne y T. Berners−Lee. Decentralization: The future of online social networking. In *W3C Wks. on the Future of Social Networking Position Papers*, 2009.

[13] P. W.L. Fong y I. Siahaan. Relationship−based access control policies and their policy languages. In *Proc. of the 16th ACM sym. on Access control models y technologies*, SACMAT '11, pages 51–60. ACM, 2011.

[14] F. Salim y J. Reid y E. Dawson. An administrative model for $UCON_{ABC}$. In *Proc.s of the Eighth Australasian Conf. on Information Security*, volume 105 of *AISC '10*, pages 32–38, 2010.

[15] S. Seong y J. Seo y M. Nasielski y D. Sengupta y S. Hangal y S.K. Teh y R. Chu y B. Dodson y M.S. Lam. Prpl: a decentralized social networking infrastructure. pages 8:1–8:8, 2010.

[16] D. M. Boyd y N. B. Ellison. Social network sites: Definition, history y scholarship. *Jnl. of Computer−Mediated Commun.*, 13:210–230, 2007.

[17] M. M. Lucas y N. Borisov. Flybynight: mitigating the privacy risks of social networking. In *Proc. of the 7th ACM wks. on Privacy in the electronic society*, WPES '08, pages 1–8. ACM, 2008.

[18] S. Jahid y P. Mittal y N. Borisov. Easier: encryption−based access control in social networks with efficient revocation. In *Proceedings of the 6th ACM Sym. on Information, Computer y Communications Security*, ASIACCS '11, pages 411–415. ACM, 2011.

[19] R.S. Sandhu y P. Samarati. Access control: Principles y Practice. *Access*, pages 40–48, 1994.

[20] M. Sastry y R. Krishnan y R. Sandhu. A New Modeling Paradigm for Dynamic Authorization in Multi−domain Systems. pages 153–158, 2007.

[21] J. Park y R. Sandhu. A Position Paper: A Usage Control (UCON) Model for Social Networks Privacy. 2000.

[22] J. Park y R. Sandhu. The $UCON_{ABC}$ usage control model. *ACM Trans. Inf. Syst. Secur.*, 7:128–174, 2004.

[23] J. Park y R. Sandhu y Y. Cheng. A user−activity−centric framework for access control in online social networks. *Internet Computing, IEEE*, 15(5):62 –65, 2011.

[24] S.C. Vimercati y S. Foresti y P. Samarati. Authorization y Access Control. *Security, Privacy and Trust in Modern Data Management*, pages 39–53, 2007.


[3] http://www.unthink.com/