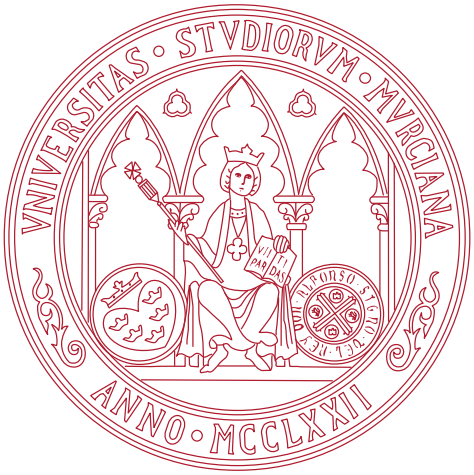
UNIVERSIDAD DE MURCIA

FACULTAD DE INFORMÁTICA

A Proposal for User's Privacy Management
in Context-Aware Systems

Propuesta para la Gestión de la Privacidad de los
Usuarios en Sistemas Sensibles al Contexto

D. Alberto Huertas Celdrán
2017



UNIVERSIDAD DE MURCIA

FACULTAD DE INFORMÁTICA

A Proposal for User's Privacy Management in Context-Aware Systems

Propuesta para la Gestión de la Privacidad de los Usuarios en Sistemas Sensibles al Contexto

Author

Alberto Huertas Celdrán

Thesis advisors

Dr. Félix Jesús García Clemente
Dr. Gregorio Martínez Pérez
Dr. Manuel Gil Pérez

Murcia, December 2016

The following PhD Thesis is a compilation of the next published articles, being the PhD student the main author in all of them:

1. Alberto Huertas Celdrán, Félix J. García Clemente, Manuel Gil Pérez, Gregorio Martínez Pérez. "SeCoMan: A semantic-aware policy framework for developing privacy-preserving and context-aware smart applications", IEEE Systems Journal, vol. 10, no. 3, pp. 1111-1124, September 2016. http://dx.doi.org/10.1109/JSYST.2013.2297707

2. Alberto Huertas Celdrán, Manuel Gil Pérez, Félix J. García Clemente, Gregorio Martínez Pérez. "PRECISE: Privacy-aware recommender based on context information for Cloud service environments", IEEE Communications Magazine, vol. 52, no. 8, pp. 90-96, August 2014. http://dx.doi.org/10.1109/MCOM.2014.6871675

3. Alberto Huertas Celdrán, Manuel Gil Pérez, Félix J. García Clemente, Gregorio Martínez Pérez. "Design of a recommender system based on users' behavior and collaborative localization and tracking", Journal of Computational Science, vol. 12, pp. 83-94, January 2016. http://dx.doi.org/10.1016/j.jocs.2015.11.010

Table of Contents

Agradecimientos/Acknowledgements iii

Resumen 1
- I Motivación y Objetivos . . . 1
- II Metodología . . . 4
- III Resultados . . . 6
- IV Conclusiones y Trabajo Futuro . . . 8

Abstract 10
- I Motivation and Goals . . . 10
- II Methodology . . . 13
- III Results . . . 14
- IV Conclusions and Future Work . . . 16

Publications composing the PhD Thesis 18

1 SeCoMan: A semantic-aware policy framework for developing privacy-preserving and context-aware smart applications 20
- I Abstract . . . 21

2 PRECISE: Privacy-aware recommender based on context information for Cloud service environments 22
- I Abstract . . . 23

3 Design of a recommender system based on users' behavior and collaborative localization and tracking 24
- I Abstract . . . 25

Bibliography 27

Agradecimientos/Acknowledgements

Agradecimientos

En primer lugar me gustaría dar las gracias a mis padres por el cariño, educación y valores que me han transmitido desde pequeño. A mi madre, María Dolores, por todo su enorme trabajo y cariño para sacar adelante a la familia. Mil gracias. A mi padre, Rufino, por su dedicación en mi educación y por los valores de esfuerzo y compromiso que me transmitió. Aunque te fuiste muy pronto, siempre serás mi ejemplo a seguir. A mi hermana, Gloria, porque siempre ha estado a mi lado en los momentos difíciles. A toda mi familia, tíos, primos y abuelos por sus muestras de cariño y ayuda todos estos años. Mil gracias a todos.

También quiero agradecer a mis amigos los buenos momentos vividos, así como el apoyo en los momentos no tan buenos. Gracias por vuestro tiempo, ayuda y consejos.

Finalmente, también me gustaría agradecer a mis directores, Félix, Gregorio, y Manuel, la posibilidad de haber aprendido de ellos valores como la perseverancia, el esfuerzo o la superación en el trabajo; sin olvidar la parte más importante de la vida, la felicidad.

Acknowledgements

First I would like to thank my parents for the love, education and values transmitted since I was a child. To my mother, María Dolores, for all her great work and love to carry out the family. Many thanks. To my father, Rufino, for his dedication in my education and for the values of effort and commitment he transmitted to me. Although you left very soon, you will always be my model. To my sister, Gloria, because she has always been at my side in the difficult moments. To all my family, uncles, cousins and grandparents for their signs of affection and help all these years. Thank you all.

I also want to thank my friends for the good times lived, as well as their support in the not so good moments. Thanks for your time, help and advices.

Finally, I would also like to thank my directors, Félix, Gregorio, and Manuel, the possibility of learning from them values such as perseverance, effort, or improvement at work; without forgetting the most important part of life, the happiness.

Resumen

I Motivación y Objetivos

Proteger la privacidad de los usuarios en sistemas de gestión de la información es un reto todavía abierto, el cual ha sido ampliamente estudiado en muchos tipos de aplicaciones [1, 2, 3]. A día de hoy, esta protección es una tarea aún más difícil de realizar debido a la evolución que han experimentado los sistemas de gestión de la información a lo largo de los últimos años. Esta evolución ha causado que los sistemas actuales deban gestionar y proteger grandes cantidades de información heterogénea y sensible en cualquier momento y lugar. En la Figura 1 se muestra la evolución de los sistemas de gestión de la información y las piezas de información más representativas que normalmente son gestionadas por dichos sistemas. Como se puede ver en la figura, esta evolución ha aumentado la cantidad de información gestionada y, por lo tanto, la complejidad del proceso de gestión de estos sistemas.

Los primeros años de los sistemas de gestión de la información estuvieron enfocados a la gestión y almacenamiento de la información en negocios y grandes compañías. Sin embargo, como resultado de las mejoras en el software y en el hardware otros nuevos paradigmas de computación han ido apareciendo, como, por ejemplo, la computación distribuida, móvil o pervasiva. Estos nuevos paradigmas han cambiado el enfoque y funcionalidad de los sistemas de gestión de la información [4]. El surgimiento de dispositivos móviles causó que los usuarios pudieran acceder a los servicios en cualquier lugar y momento. Además, estos dispositivos introdujeron un nuevo elemento clave para los sistemas de gestión de la información: la localización de los usuarios. A los sistemas que proporcionan información considerando la localización de los usuarios se les conoce, del inglÃ©s, como *location-based services* [5]. Algunos de estos sistemas van un paso más allá y son capaces de proporcionar servicios avanzados capaces de predecir movimientos de los usuarios, o incluso el comportamiento futuro de éstos. Sin embargo, estos servicios basados en localización también incrementaron la complejidad de la protección de la privacidad de los usuarios. La información más importante gestionada por los servicios basados en localización se muestra en el triángulo azul de la Figura 1.

En los primeros años de la década de los 90, también influenciado por los progresos tanto en hardware como en software, surgió un paradigma de computación llamado, del inglés, *pervasive computing*. El concepto *pervasive* fue definido por Weiser [6] como la integración de dispositivos de computación en la vida de los usuarios sin que ésta se viera afectada. Concretamente, este paradigma de computación estaba enfocado a las personas, en lugar de centrarse en los dispositivos de computación y sus problemas técnicos. La información de movilidad de los usuarios,

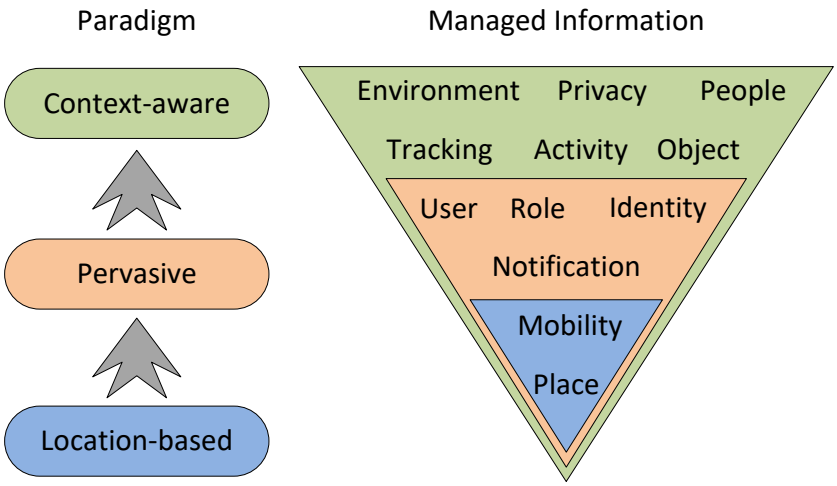


Figure 1: Evolución de los sistemas de gestión de la información

proporcionada por los servicios basados en localización, fue un aspecto esencial para el éxito de este paradigma. En este sentido, los sistemas de gestión de la información no solo consideraban la localización de los usuarios, sino también información sobre la vida de los mismos. Un ejemplo de la información gestionada por este paradigma se muestra en los triángulos naranja y azul de la Figura 1. Los principales objetivos de la computación pervasiva fueron: el uso efectivo y eficiente de los elementos que componían los lugares donde estaban los usuarios; la invisibilidad o completa desaparición de los dispositivos computacionales, desde la perspectiva de los usuarios; la gestión del número de elementos que componían el entorno del usuario; y la sensibilidad al contexto que los rodeaba.

Hoy en día, el concepto *sensibilidad del contexto* (del inglés *context-awareness*) [7] es el núcleo de la computación pervasiva, y en donde esta tesis doctoral está enfocada. *Context-awareness* es un paradigma móvil donde los servicios descubren la información del contexto o entorno en el cual los usuarios están localizados, y adaptan sus comportamientos teniendo en cuenta esta información sin la intervención de dichos usuarios. Las soluciones sensibles al contexto utilizan servicios basados en la localización para obtener la posición de los usuarios. Una vez que la localización es conocida, estos sistemas proporcionan información acerca de las personas, objetos y elementos que componen el contexto o entorno donde el usuario está ubicado. En la literatura actual podemos encontrar varias definiciones del término contexto. La primera apareció en 1994 y fue realizada por Schilit et al. [8]. Estos autores describieron el contexto como la localización e identidades de las personas y objetos cercanos al usuario, así como los cambios de estos elementos. Después de esta primera definición, varios autores incluyeron nuevos aspectos como, por ejemplo, las identidades y el tiempo (Ryan et al. [9]), estados emocionales y centros de atención (Dey [10]), dimensiones del contexto (Prekop y Burnett [11] y Gustavsen en 2002 [12]) y cualquier dato del entorno (Tajd and Ngantchaha [13]). En esta tesis doctoral, nosotros asumimos que el contexto debería considerar la localización de las personas y los objetos ubicados cerca del usuario al que se le quieren proporcionar ciertos servicios, las identidades de esos objetos y de las personas, la información relacionada con el contexto o entorno donde el usuario está localizado, así como cualquier cambio que pudiera acontecer en los aspectos anteriores. Como ejemplo, el triángulo verde de la Figura 1 muestra una parte de la información más importante gestionada por los sistemas sensibles al contexto. Como se puede ver, ese triángulo también considera la información gestionada por los sistemas pervasivos y los basados en la localización.

Durante los últimos años se han propuesto muchos servicios sensibles al contexto con el fin de facilitar la vida de los usuarios. A pesar de que el concepto *contexto* fue propuesto en 1994, es ampliamente aceptado que la primera solución sensible al contexto fue propuesta por Want el al. en 1991 [14]. En esta propuesta, los autores introdujeron un nuevo sistema para localizar a las personas en un entorno de oficinas llamado *Active Badge*. Este sistema era capaz de saber la localización de los usuarios y desviar las llamadas telefónicas al teléfono más cercano al usuario al que iba destinada la llamada. La localización de los usuarios era conocida gracias a que éstos portaban unos dispositivos llamados *badges*, los cuales transmitían señales de radio a un sistema de localización centralizado. Después de esta solución se han realizado muchas otras propuestas en diferentes tópicos. Por ejemplo, Wood et al. [15] propuso una solución que era capaz de transportar entornos de computación entre diferentes computadoras que tuvieran un navegador con Java. Usando esta solución, los usuarios ya no tenían que llevar consigo sus computadoras puesto que eran capaces de ejecutar sus aplicaciones en cualquier otra máquina cercana. Estos sistemas sensibles al contexto abrieron nuevas posibilidades a los usuarios en cuanto a la adquisición de servicios personalizados obteniendo la información del contexto, especialmente, en aplicaciones donde la movilidad de los usuarios incrementa su utilidad. Navegadores para coches, servicios de emergencias o recomendadores son ejemplos de soluciones sensibles al contexto donde la movilidad de los usuarios incrementa su usabilidad.

En referencia a los servicios basados en localización comentados previamente, los sistemas recomendadores están ganando gran popularidad debido a la importante ayuda que estas soluciones proporcionan, recomendando objetos o servicios que probablemente no hubieran sido descubiertos por los propios usuarios. Las recomendaciones sensibles al contexto [16] consideran aspectos como la distancia entre usuarios y objetos, o los movimientos de éstos a la hora de sugerir objetos que podrían ser de su interés. A pesar del progreso que han experimentado estas soluiones, todavía quedan retos sin resolver en este campo a la hora de proporcionar recomendaciones más precisas, además de dar solución a problemas bien conocidos como el *data sparsity* y el *cold-start* [17, 18]. Concretamente, el problema de la "escasez de datos" (del inglés data sparsity) surge del hecho de que los usuarios, por norma general, solo valoran un pequeño número de objetos y, por lo tanto, la matriz que almacena estas valoraciones carece de información. Por otro lado, el problema del "arranque en frío" (del inglés cold-start) hace referencia a la dificultad de proporcionar recomendaciones a usuarios que son nuevos en el sistema, y que no han valorado todavía alguno de los objetos. Este problema también lo tienen objetos nuevos que previamente no han sido valorados.

Los sistemas sensibles al contexto, como cualquier sistema de gestión de la información, tienen diferentes retos orientados a la privacidad [19]. Sin embargo, la mayoría de los sistemas sensibles al contexto que podemos encontrar en la literatura no consideran la protección de partes importantes de la información de los usuarios [20]. La identidad y la información personal son piezas muy importantes que deben ser protegidas por estos sistemas en muchos casos. Además, la inclusión de la localización de los usuarios ha incrementado la complejidad del proceso de protección. Por un lado, los sistemas sensibles al contexto deben gestionar la información importante de los usuarios como, por ejemplo, sus localizaciones, identidades, actividades e información acerca del contexto o lugar donde ellos están. Por otro lado, los sistemas sensibles al contexto deben permitir a los usuarios decidir qué quieren hacer con su información personal sobre cúando, dónde, cómo y a quién quieren revelarla.

A lo hora de gestionar la información, y permitir a los usuarios la protección de ésta, las técnicas basadas en web semántica [21] son una manera prometedora de llevar a cabo la gestión y protección de la información de los usuarios y el contexto en el que están. Concretamente, tanto los usuarios como los sistemas pueden proteger la información haciendo uso de reglas semánticas que definen políticas de privacidad. Estas políticas permiten revelar información al

destino deseado, en el momento, lugar y tiempo establecido por el usuario. Por otro lado, las ontologías [22] permiten a los sistemas sensibles al contexto representar la información de tal forma que es posible inferir nuevo conocimiento haciendo uso de razonadores semánticos. Además, las ontologías también permiten la compartición de conocimiento entre sistemas independientes y el uso de razonamiento semántico para ofrecer servicios avanzados a los usuarios. Debido a ello, las técnicas basadas en web semántica pueden ser empleadas para llevar la gestión de complejos sistemas sensibles al contexto que tienen en cuenta la privacidad de los usuarios, permitiendo las características avanzadas que estos sistemas necesitan y que no han sido totalmente resueltas por las soluciones encontradas en el estado del arte.

Debido a los retos comentados anteriormente, sobre los sistemas sensibles al contexto que tienen en cuenta la privacidad de la información de los usuarios, el principal objetivo de esta tesis doctoral consiste en investigar acerca de la computación pervasiva, los sistemas sensibles al contexto y la privacidad de la información para proponer soluciones sensibles al contexto innovadoras usando técnicas basadas en web semántica. En particular, para llevar a cabo el objetivo principal comentado más arriba, se han llevado a cabo una serie de acciones específicas descritas a continuación:

- Estudiar y analizar la evolución de los sistemas de gestión de la información, desde soluciones basadas en la localización hasta sistemas sensibles al contexto, así como también el impacto de la privacidad de los usuarios en estos sistemas.
- Estudiar el estado del arte de sistemas que protegen la privacidad de la información y analizar cómo las técnicas basadas en web semántica pueden ayudar en la gestión y protección de la información considerada por los sistemas sensibles al contexto.
- Proponer, implementar y validar un sistema basado en la localización y sensible al contexto que intercambia y protege entre usuarios sus localizaciones haciendo uso de técnicas basadas en web semántica.
- Diseñar e implementar una solución sensible al contexto capaz de intercambiar entre usuarios y servicios información personal de los usuarios y del contexto en el que están, teniendo en cuenta la privacidad de dicha información.
- Estudiar y analizar el estado del arte de los sistemas recomendadores que consideran información sensible al contexto a la hora de mejorar las recomendaciones proporcionadas a los usuarios.
- Diseñar, implementar y validar un sistema recomendador sensible al contexto capaz de recomendar objetos localizados en el mismo contexto o entorno donde se encuentra el usuario, además de proporcionar valoraciones automáticas teniendo en cuenta los movimientos del usuario después de recibir las recomendaciones.

II Metodología

Esta tesis doctoral ha sido realizada siguiendo un proceso científico basado en el estudio del estado del arte y el análisis de los resultados proporcionados por el desarrollo de los sistemas sensibles al contexto existentes. Siguiendo el primer objetivo definido en la sección anterior, esta tesis doctoral comenzó con el estudio y análisis del estado del arte de los sistemas de gestión de la información. Concretamente, los esfuerzos se centraron en los sistemas sensibles al contexto y basados en la localización que consideran la privacidad de la información de los usuarios. Después de realizar dicho estudio se llegó a la conclusión de que, a pesar de los innumerables

avances realizados por las soluciones existentes, la mayoría de ellas no protegen la privacidad de la información de los usuarios, o no tienen en cuenta la protección de piezas importantes de dicha información.

Para encontrar la mejor forma de proteger la información de los usuarios en sistemas sensibles al contexto, y en relación con el segundo objetivo de esta tesis doctoral, se estudió y analizó el estado del arte de soluciones que protegen la privacidad de la información de los usuarios en este tipo de sistemas. Este estudio mostró que la mayoría de las soluciones no gestionan dinámicamente la información, ni permiten a los usuarios proteger partes sensibles e importantes de su información. La principal conclusión extraída de dicho análisis fue que los sistemas basados en políticas son una forma prometedora para gestionar dinámicamente la privacidad de la información de los usuarios. Siguiendo el segundo objetivo de esta tesis, también se analizó el estado del arte de las tecnologías orientadas a la web semántica. En este sentido se evaluaron diferentes lenguajes para el modelado de la información haciendo uso de ontologías. También se compararon diferentes lenguajes para la definición de políticas encargadas de proteger la privacidad de los usuarios de forma dinámica, así como diferentes razonadores lógicos encargados de inferir nuevo conocimiento. Este estudio reveló que durante los últimos años las tecnologías orientadas a la web semántica han evolucionado lo suficiente como para permitirnos su uso en sistemas sensibles al contexto. Concretamente, éstas pueden ser utilizadas como mecanismo para modelar la información del contexto, definir las políticas de privacidad de los usuarios, inferir nuevo conocimiento a través de razonadores semánticos y compartir la información entre sistemas independientes. En la literatura se pueden encontrar diferentes propuestas orientadas a la web semántica que hacen uso de políticas, ontologías y razonadores semánticos para gestionar y controlar la información en diferentes tópicos [23, 24]. A la hora de reducir los problemas comentados anteriormente, y enfocado en el tercer objetivo de esta tesis, se ha diseñado, implementado y evaluado un *framework* sensible al contexto y basado en la localización que permite a los usuarios proteger la privacidad de su información (Capítulo 1). La solución presentada propone e implementa una arquitectura basada en técnicas de web semántica. Dicha arquitectura contiene los componentes necesarios para gestionar y proteger la información de los usuarios y sus contextos. La información ha sido modelada de forma estructurada haciendo uso de ontologías. Además, se ha definido un conjunto de políticas de privacidad encargadas de proteger la localización de los usuarios en los distintos contextos. La información gestionada por las ontologías, y protegida por las políticas, ha sido utilizada en un caso de uso que muestra la utilidad de la solución propuesta. Finalmente, para la evaluación de esta solución se ha llevado a cabo una batería de experimentos que muestran su rendimiento.

Durante la investigación llevada a cabo, y orientada a la privacidad en soluciones sensibles al contexto, se encontró una falta de propuestas donde los usuarios son capaces de proteger su información no solo respecto a otros usuarios, sino también con respecto a servicios. En este sentido, y relacionado con el cuarto objetivo definido en esta tesis doctoral, se propuso, diseñó, implementó y validó una solución sensible al contexto y basada en la localización encargada de proteger la privacidad de la información y proporcionar recomendaciones considerando la información que los usuarios proporcionan a los servicios. Proporcionar recomendaciones sensibles al contexto y basadas en la localización requiere tener en cuenta diferentes aspectos como, por ejemplo, la gran cantidad de información contextual que debe ser modelada, los requisitos de procesamiento necesarios para gestionar la información contextual, así como la necesidad de ofrecer servicios que son ejecutados en sistemas federados pertenecientes a diferentes organizaciones. Teniendo en cuenta estas necesidades, se propuso una solución orientada al paradigma *Mobile Cloud Computing* (MCC) que permite a los usuarios gestionar su privacidad, principalmente, con respecto a los servicios (Capítulo 2). En primer lugar, se definió un caso de uso donde se mostraron los problemas de privacidad que los usuarios de estos sistemas podían encontrar

en su día a día. Para resolver los problemas planteados en dicho caso de uso se diseñaron y desplegaron varias políticas encargadas de proteger partes sensibles e importantes de la información de los usuarios con respecto a servicios concretos. A la hora de realizar la gestión de dichas políticas y la información de los usuarios y de los contextos se definió una arquitectura orientada al paradigma MCC. Finalmente, también se diseñó una aplicación móvil encargada de permitir a los usuarios controlar su privacidad, creando, borrando y modificando sus políticas.

En la línea de la propuesta anterior, y para llevar a cabo el quinto objetivo de esta tesis doctoral, se ha estudiado el estado del arte de sistemas recomendadores sensibles al contexto. El análisis realizado acerca de los recomendadores encontrados en la literatura ha mostrado que la habilidad de combinar la localización y los movimientos de los usuarios, junto con otros aspectos como las preferencias y valoraciones de éstos, o las propiedades de los objetos, es una tarea compleja que puede ayudar a proporcionar recomendaciones precisas. En este sentido, también se han descubierto varios retos sin resolver relacionados con la mejora de problemas importantes como el *data sparsity* y el *cold-start*. Entre los retos encontrados, destacar la forma de encontrar usuarios similares teniendo en cuenta las valoraciones de éstos, la forma de crear perfiles de usuarios y clasificar los objetos y cómo hacer uso de las localizaciones y rutas de los usuarios para recomendar objetos. Como último objetivo de esta tesis, siguiendo los retos comentados y con la intención de reducir los problemas previamente definidos, se propuso un sistema recomendador capaz de ofrecer recomendaciones sensibles al contexto y proporcionar valoraciones automáticas. Dichas valoraciones se realizaban teniendo en cuenta los movimientos de los usuarios después de recibir las recomendaciones (Capítulo 3).

III Resultados

Esta tesis doctoral es una compilación de un conjunto de publicaciones, por lo que los resultados están esencialmente detallados en los artículos que la componen. Siguiendo la metodología definida en la sección anterior, para llevar a cabo los tres primeros objetivos de esta tesis se diseñó, implementó y validó una solución sensible al contexto que permite el desarrollo de aplicaciones teniendo en cuenta la privacidad de la localización de los usuarios. Los resultados derivados de la evaluación del estado del arte, así como la definición e implementación de un sistema sensible al contexto, fueron presentados en la revista IEEE Systems Journal, Special Issue on Intelligent Internet of Things, en un artículo títulado "SeCoMan: A Semantic-Aware Policy Framework for Developing Privacy-Preserving and Context-Aware Smart Applications" [25]. En dicho artículo se propone un sistema que proporciona soporte para desarrollar aplicaciones inteligentes sensibles al contexto preservando la privacidad de los usuarios en una visión orientada a la web semántica. Este sistema es capaz de obtener la información del contexto en el que se encuentran los usuarios, modelar y proteger la información de los contextos y de los usuarios, así como proporcionar aplicaciones sensibles al contexto. Para realizar este proceso, se ha diseñado e implementado una arquitectura orientada a la web semántica [26]. La información de los usuarios y los contextos se modela haciendo uso de una colección de ontologías definidas en OWL 2 [27], mientras que la información de los usuarios es protegida usando políticas, las cuales son definidas en SWRL [28]. Estas políticas permiten a los usuarios compartir sus localizaciones con los usuarios que ellos desean, con la precisión que quieren, y en el lugar y tiempo establecidos por ellos. Finalmente, la información sobre los contextos y los usuarios se les proporciona a las aplicaciones sensibles al contexto haciendo uso de *queries* definidas en SPARQL [29]. En esta publicación también se han incluido resultados de la implementación y evaluación de un prototipo en el contexto de un supermercado. El contexto del supermercado ha sido elegido debido a la cantidad y riqueza de diferentes servicios que pueden ser proporcionados por dicho contexto. Finalmente, un análisis del rendimiento muestra tiempos razonables para la gestión,

protección y provisión de la información tanto de los usuarios como de sus contextos.

Teniendo en cuenta los dos primeros objetivos definidos en esta tesis doctoral, y para acometer el cuarto objetivo, se ha continuado con la investigación de la protección de la información de los usuarios en soluciones sensibles al contexto. Como resultado de esta investigación se propuso e implementó una plataforma orientada a proteger la información de los usuarios con respecto a los servicios. Este resultado se definió en un artículo titulado "PRECISE: Privacy-Aware Recommender Based on Context Information for Cloud Service Environments" [30], el cual fue publicado en la revista IEEE Communications Magazine, Feature Topics Issue on Context-Aware Networking and Communications. En este artículo se define un sistema que protege la privacidad de la información y proporciona recomendaciones sensibles al contexto considerando la información que los usuarios quieren revelar a servicios determinados. Haciendo uso de la solución propuesta, los usuarios pueden liberar sus localizaciones a servicios concretos, ocultar sus posiciones a usuarios específicos, enmascarar sus localizaciones proporcionando posiciones falsas tanto a servicios como a otros usuarios, establecer la precisión y cercanía con la que quieren liberar sus localizaciones y preservar su anonimato a determinados servicios. Para realizar dichas tareas se ha diseñado y desplegado una arquitectura orientada al paradigma MCC compuesta de tres capas. En dicha arquitectura, los servicios están localizados en la capa superior. El elemento central es un *middleware* que se encarga de gestionar el contexto, proteger la información de los usuarios y es independiente de los sistemas que proporcionan la información de localización. En este trabajo también se ha incluido una comparación entre las soluciones sensibles al contexto que pueden encontrarse en la literatura, resaltando las diferencias principales con esta propuesta. Entre esas diferencias, se destaca la cantidad de políticas de privacidad basadas en la localización que los usuarios de nuestra solución pueden utilizar a la hora de controlar su información de localización.

Finalmente, los resultados obtenidos después de seguir la metodología definida para el quinto y sexto objetivo consisten en un sistema recomendador sensible al contexto. Dicho sistema fue publicado en la revista Journal of Computational Science bajo el título "Design of a Recommender System Based on Users' Behavior and Collaborative Location and Tracking" [31]. En este artículo se ha diseñado un algoritmo recomendador sensible al contexto con soporte para valoraciones automáticas. El algoritmo recomendador propuesto combina diferentes enfoques para ordenar los objetos sugeridos. Concretamente, considera las valoraciones proporcionadas por usuarios similares al que va a recibir la recomendación (enfoque *Collaborative Filtering*); las propiedades de los objetos sugeridos como, por ejemplo, el precio o el tipo (enfoque *Content Based Filtering*); y la localización y movilidad de los usuarios y objetos (enfoque *Context-Aware*). Además, la solución propuesta proporciona valoraciones automáticas teniendo en cuenta el comportamiento de los usuarios después de recibir las recomendaciones. Aspectos como el tiempo y la localización de los usuarios y los objetos son considerados a la hora de medir el interés de los usuarios por los objetos recomendados. La gestión de la información en el sistema recomendador se realiza haciendo uso de técnicas de web semántica. En este sentido, y como extensión de la segunda propuesta realizada en esta tesis doctoral, se ha diseñado una ontología para modelar la información del algoritmo recomendador y valorador. Además, se ha analizado el impacto de los aspectos considerados en los procesos de recomendación y valoración, así como la efectividad de éstos. Los resultados obtenidos demuestran mejoras con respecto a otras soluciones en métricas como la precisión, *recall* y *F-measusure*. Además, se ha demostrado que los aspectos y parámetros considerados por el algoritmo valorador son útiles a la hora de generar valoraciones implícitas y automáticas.

IV Conclusiones y Trabajo Futuro

El auge de los dispositivos móviles ha provocado una increíble evolución en los sistemas de gestión de la información. Hoy en día, la mayoría de sistemas de gestión de la información son consumidos en cualquier momento y lugar. Debido a este hecho, la localización de los usuarios ha tomado gran importancia a la hora de proporcionar servicios próximos a los usuarios. A los servicios que hacen uso de la localización de los usuarios para proporcionar información acerca de los elementos ubicados en el mismo entorno o contexto se les conoce como servicios sensibles al contexto. El surgimiento de este tipo de servicios ha hecho que la complejidad del proceso de protección de la información de los usuarios aumente significativamente. Los servicios sensibles al contexto gestionan información muy apreciada que debería ser protegida como, por ejemplo, la localización de los usuarios, sus actividades, identidades y patrones de comportamiento. En caso de que esta información no fuera protegida, cualquier usuario o proveedor de servicios podría obtener dicha información y hacer un mal uso de la misma.

La gestión de la privacidad de la información de los usuarios, en sistemas sensibles al contexto y basados en la localización, es un reto que aún sigue abierto y el cual requiere de ciertos esfuerzos para ser solucionado. Los sistemas sensibles al contexto deberían permitir a los usuarios controlar qué información quieren revelar, cuándo y cómo la información debe ser revelada, y a quién. Técnicas basadas en web semántica son una prometedora forma de llevar a cabo la gestión y protección de la información personal y del contexto. Esta tecnología permite el modelado estructural de la información, intercambiar información entre sistemas independientes, definir políticas de privacidad para proteger la información e inferir nuevo conocimiento teniendo en cuenta la información de las ontologías y las políticas definidas en el sistema.

Teniendo en cuenta los hechos anteriores, en esta tesis doctoral han sido propuestos, analizados e implementados un conjunto de soluciones orientadas a la mejora de la privacidad de los usuarios en sistemas sensibles al contexto basados en la localización. Para este fin se ha propuesto una solución que permite el desarrollo de aplicaciones sensibles al contexto que consideran la privacidad de la localización de los usuarios. La solución propuesta es un middleware llamado *SeCoMan* que permite a los usuarios definir sus políticas de privacidad para controlar dónde, cuándo, cómo y a quién sus localizaciones son reveladas. En este sentido, los usuarios no tienen que confiar en las aplicaciones sensibles al contexto, para lo cual nuestra solución define un conjunto de *queries* predefinidas que proporcionan información a las aplicaciones sensibles al contexto. En esta solución se ha diseñado también un conjunto de ontologías que modelan la información del espacio y del contexto de un supermercado.

Adicionalmente, se ha propuesto una solución sensible al contexto orientada al paradigma MCC, la cual se encarga de proteger la información de los usuarios no solo con respecto a otros usuarios, sino también con respecto a los servicios. A la hora de demostrar la utilidad de la solución propuesta, se ha desarrollado un sistema recomendador capaz de proporcionar recomendaciones sensibles al contexto que consideran la información revelada por los usuarios a los servicios que proporcionan las recomendaciones. Usando este sistema, los usuarios pueden ocultar sus identidades a determinados servicios, ocultar sus localizaciones y proporcionar posiciones falsas, entre otras cosas.

Finalmente, la última contribución de esta tesis consiste en un sistema recomendador sensible al contexto que combina diferentes enfoques para proporcionar recomendaciones precisas, así como reducir problemas bien conocidos como el *data sparsity* y el *cold-start*. En este sentido, la solución propuesta combina las valoraciones de usuarios similares al que se le está proporcionando el servicio, información sobre los objetos sugeridos como el precio o el tipo, y la información sobre el contexto como la distancia entre los usuarios y los objetos, además de su movilidad. Por otro lado, también se ha propuesto un algoritmo valorador que proporciona valoraciones automáticas

teniendo en cuenta el comportamiento de los usuarios después de recibir las recomendaciones. Los experimentos realizados han mostrado evidencias de la eficacia de la solución propuesta, y cómo los parámetros sensibles al contexto usados en el recomendador mejoran la precisión de las recomendaciones.

Esta tesis doctoral mejora algunos de los problemas encontrados en la literatura relativos a los sistemas sensibles al contexto. En este sentido, la primera contribución se centró en permitir a los usuarios controlar la liberación de su localización con respecto a otros usuarios mediante la definición de políticas. La segunda propuesta de esta tesis consistió en un sistema recomendador sensible al contexto que permitía a los usuarios proteger no solo su localización, sino otras partes sensibles de su información y no solo con respecto a otros usuarios, sino también con respecto a servicios. Finalmente, la última contribución fue un sistema recomendador sensible al contexto, encargado de combinar diferentes enfoques con la movilidad y localización de los usuarios para mejorar las recomendaciones y valoraciones automáticas.

Como trabajo futuro de esta tesis, se plantea considerar la protección de la privacidad de los usuarios cuando éstos se mueven entre distintos contextos y hay un intercambio de información entre los contextos (escenario intercontexto). Esta situación conlleva nuevas preguntas que deberían ser consideradas como, por ejemplo, cómo los usuarios gestionarían y protegerían la información que quieren compartir, quién gestionaría la privacidad de la información de los contextos y qué información podría ser intercambiada entre contextos independientes.

Otra futura línea de trabajo consiste en ayudar a los usuarios sin suficientes conocimientos técnicos sobre la privacidad a la hora de proteger su información. En este sentido, y dependiendo del contexto en el que estén localizados los usuarios, éstos recibirían varios perfiles sensibles al contexto compuestos de políticas de privacidad que protegerían su información en el contexto en el que se encuentren.

Abstract

I Motivation and Goals

Preserving the privacy of users' information in information management systems is an open challenge that has been widely studied in multiple application domains [1, 2, 3]. Nowadays, this protection is a task still more difficult to tackle due to the evolution experienced by information management systems over the last years. This evolution has caused that current systems must manage and protect a large amount of heterogeneous and sensitive information at anytime and anyplace. In Figure 1 it is shown the evolution of information management systems and the most representative pieces of information usually managed by them. As it can be seen, the depicted evolution has augmented the amount of managed information and therefore the complexity of the management and protection processes.

The early days of information management systems were focused on the management and storage of business information in large companies. However, as a result of improvements in software and hardware, new computing paradigms appeared as distributed, mobile, or pervasive computing, so shifting the focus and functionality of information management systems [4]. The rise of mobile devices caused that users could access services at anyplace and anytime. Furthermore, these devices introduced a new key element in information management systems: the location of users. Systems that provide information considering the user's location are called *location-based services* [5]. Some of these systems go a step further so as to provide useful services predicting the potential future movements and behavior of users. However, these location-based services have also increased the complexity of the protection of the users' privacy. Users' locations could be tracked without the users' consent, and this information could be used in a potential malicious way. The most representative information managed by location based-services is depicted in the blue triangle of Figure 1.

At the beginning of the '90s emerged the *pervasive computing paradigm*, also due to the progress achieved in hardware and software elements. The pervasive concept was introduced by Weiser [6] as the seamless integration of devices into the users' everyday life. Specifically, the pervasive paradigm made people the central focus rather than computing devices and technical issues. The users' mobility records were an essential piece of information for this paradigm and they were provided by the location-based services. In this sense, information management systems considered not only the users' location, but also information about the users' life. One example of the information managed by this paradigm is shown in the orange and blue triangles of Figure 1. The main goals of pervasive computing are the effective and efficient use of the

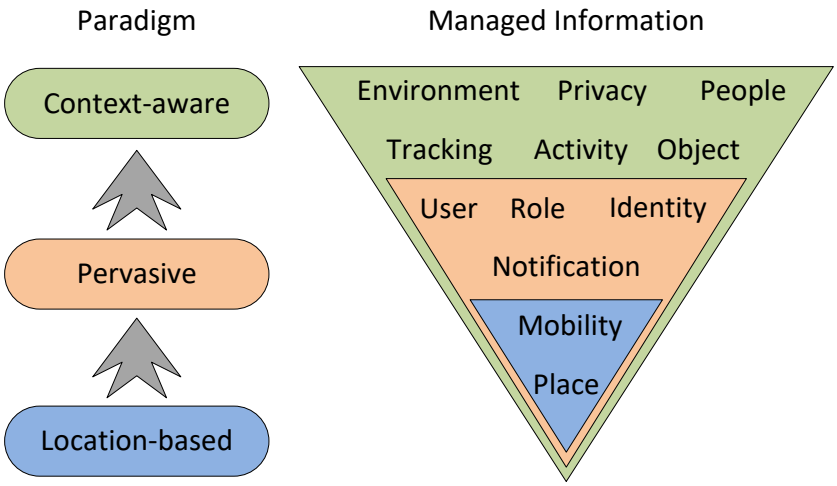


Figure 1: Evolution of information management systems

elements that compose the spaces where users are, the invisibility or complete disappearance of computing technology from the user's perspective, the number of elements that compose the environment, and the context-awareness.

Nowadays, the *context-awareness* concept [7] is the core of pervasiveness, about which the PhD Thesis at hand is focused on. Context-awareness is a mobile paradigm where services discover the information of the context or environment in which users are located, and adapt their behavior taking into account that information without users' interaction. It is important to notice that users do not interact with context-aware systems, but they consent the acquisition and management of their information. Context-aware solutions use location-based systems so as to obtain the users' location with which to gather information about the people, objects, and elements that compose the context or environment in which the users are located. In the literature, we can find several definitions of context. The first one appeared in 1994 and was made by Schilit et al. [8]. They described context as location, identities of nearby people, objects, and changes to those objects. After that, several authors included new aspects like, for example, identity and time (Ryan et al. [9]), emotional states and focus of attention (Dey [10]), context dimensions (Prekop and Burnett [11], and Gustavsen [12]), and any environmental data (Tajd and Ngantchaha [13]). In this PhD Thesis, we assume that context should consider the location of people and objects located close to the target user, the identities of these objects and people, the information related to the context or environment in which the target is located, and the changes of the information modeled by the previous three aspects. As an example, the green triangle of Figure 1 shows a part of the most important information managed by context-aware systems. As seen, this triangle considers the information managed by pervasive and location-based paradigms.

During the last years, many context-aware services have been proposed in order to make life easier. Despite the context term was proposed in 1994, it is commonly agreed that the first context-aware solution found in the literature was proposed by Want et al. in 1991 [14]. They introduced a novel system for the location of people in an office environment called Active Badge. This system was able to know the location of users in order to forward phone calls to the phones close to the user. The users' location was known because users wore badges transmitting signals to a centralized location system. After that, many different solutions have been proposed in different topics, as the one presented by Wood et al. in [15], for example. They described a "teleporting" solution, which was able to make the user' environment available in any computer

running a web browser with Java. By using this solution, users did not have to carry any computing platform and they were able to execute their applications on any nearby machine. These context-aware systems opened up new possibilities to users in terms of acquiring custom services by gathering context information, especially in applications where the high mobility of users increased their usability. Car navigation systems, emergency services, or recommender systems are well-known examples of context-aware solutions where the mobility of users increases their usability.

Regarding the location-based services commented earlier, recommender systems are becoming popular as they can help users to find items that may not have been found by users themselves. Context-aware recommendations [16] consider the distance between users and items as well as their subsequent movements change of the users' physic location in a given place, in order to suggest items to users who might be interested. Despite the progress made by the recommender systems found in the literature, there are open challenges in this topic in order to provide more accurate recommendations, and reduce well-known problems of these systems like the data sparsity and cold-start [17, 18]. Specifically, data sparsity arises from the phenomenon that users, in general, rate only a limited number of items and therefore the reported matrix of user-item ratings is usually very sparse. On the other hand, the cold-start problem refers to the difficulty in bootstrapping the recommender systems for new users or new items.

Context-aware systems, like any other kind of information management system, face different challenges regarding privacy [19]. Nonetheless, we can find many context-aware systems in the literature, although the majority of them do not consider the protection of important sensitive pieces of the contexts and users' information [20]. Identities and personal information are valuable pieces of information that should be protected by these systems in most cases. Furthermore, the inclusion of the users' location has increased the complexity of the protection process. On one hand, context-aware systems should manage sensitive information such as, for example, the location of users, their identities, their activities, and information about the context in which they are located. On the other hand, context-aware solutions should allow users to decide when, where, how, and to whom reveal the previous information.

In order to manage the information and allow users to protect it, semantic web techniques [21] are a promising way to accomplish the management and protection of contextual and personal information in context-aware systems. Specifically, users and systems can protect their information by using semantic rules to define privacy-policies. These policies will let reveal information to the right destination, at the right moment, place, and time. On the other hand, ontologies [22] allow context-aware systems to represent the information in a way that it is possible to infer new knowledge by using semantic reasoners. Furthermore, ontologies also allow sharing knowledge between independent systems and using semantic reasoning about the context to offer advanced services to customers. Thus, semantic web techniques can be employed to improve the information management in complex privacy-preserving and context-aware systems, which has not been fully addressed yet in the state of the art.

Due to the challenges of privacy-preserving and context-aware systems highlighted above, the main objective of this PhD Thesis consists on investigating the topics of pervasive computing, context-awareness, and privacy of the information in order to propose novel context-aware solutions by using semantic web techniques. In particular, the specific goals pursued within this thesis, and derived from the main objective described above, are the following ones:

- Study and analyze the evolution of information management systems from location-based solutions to context-aware systems, as well as the impact of the users' privacy in these systems.
- Study the state of art of privacy-preserving solutions, and analyze how web semantic

techniques can help in managing and protecting the information considered by the context-aware systems.

- Propose, implement, and validate a location-based and context-aware system in charge of exchanging and protecting the users' location by considering semantic web techniques.
- Design and implement a context-aware solution capable of exchanging in a privacy-preserving way personal and contextual information between users and services.
- Study and analyze the state of the art of recommender systems that consider context-aware information in order to improve recommendations.
- Design, implement, and validate a context-aware recommender system in charge of providing context-aware recommendations about items located close to the target user, as well as providing implicit or automatic ratings taking into account the users' movements after receiving recommendations.

II Methodology

This PhD Thesis has been conducted by following a scientific process based on the study of the state of the art and the analysis of the results provided by the development of the existing context-aware solutions. In order to accomplish the first objective defined in the previous section, this PhD Thesis started studying and analyzing the current state of the art of information management systems. Specifically, we focused our efforts on location-based and context-aware solutions that consider the privacy of the users' information. After this study, we realized that despite the countless advances made by existing context-aware solutions, the majority of them do not protect the privacy of the users' information, or they have not been taking into consideration in their design the protection of important pieces of sensitive information.

In order to find the best way to protect the users' information in context-aware systems, and in relation to the second goal defined in this thesis, we studied and analyzed the state of the art of privacy-preserving solutions within this kind of systems. With this study, we discovered that the majority of solutions do not manage dynamically the information nor provide users with effective means to protect important pieces of sensitive information. The main conclusion of this analysis was that systems based on policies are a promising way to manage the privacy of the users' information dynamically. Following the second goal of this thesis, we also started analyzing the status of the semantic web paradigm. In this sense, we evaluated different ontology languages in order to model in a formal way the information about contexts and users. We also compared several policy languages to define privacy-preserving policies that control the users' information in a dynamic way, as well as different semantic reasoners to infer new knowledge by considering ontologies and policies. The conclusion of this study revealed that web semantic technologies have evolved enough to be used as a mechanism to model the contextual information, to define policies that protect the users' information to infer new knowledge by means of semantic reasoners, and to share information between independent systems. In the literature, it can be found several proposals oriented to the semantic web that use policies, ontologies, and reasoners to manage and control the information in different topics [23, 24]. In order to reduce the previous drawbacks and accomplish the third goal defined in this thesis, we have designed, implemented, and evaluated a location-based and context-aware framework in charge of allowing users to protect the privacy of their information (Chapter 1). Our solution proposes and implements an architecture based on web semantic techniques, which contains the components needed to manage the information about users and contexts in a privacy-preserving way. The

information has been modeled in a formal way by using ontologies and a set of privacy policies has been defined in order to protect the users' location. The information managed by the ontology and protected by the policies has been considered in a use case where the usefulness of our solution has been shown. Finally, the evaluation of our solution has been made by designing a battery of experiments that show the performance of our solution.

During the research carried out to devise the privacy in a context-aware solution, we also found a lack of proposals where users are able to protect their privacy not only regarding other users, but also services. In this sense, and related to the fourth goal proposed in this thesis, we have proposed, designed, implemented, and validated a privacy-preserving and context-aware solution that provides recommendations by considering the information that users want to reveal to given services. Providing this kind of context-aware recommendations based on location requires the consideration of different aspects, such as the large amount of data needed to shape the context-aware information, the processing power requirements demanded to manage the contextual information, and the need to offer services that run on federated systems spanning different organizations. To accomplish these requirements, we proposed a solution oriented to the Mobile Cloud Computing (MCC) paradigm that allows users to manage their privacy, mainly regarding services (Chapter 2). To this end, we have defined a running example were the privacy concerns of users are depicted. In order to provide a solution to the problems explained in the use case, we have designed and deployed an extensible set of privacy policies that protect sensitive pieces of information regarding services. To manage these policies and the information about users and context, we have defined an architecture oriented to the MCC paradigm. Finally, we also designed a mobile application to allow users to control their privacy by creating, deleting, and modifying their privacy policies.

In the line of our previous proposal, and in order to accomplish the fifth objective of this thesis, we have studied the current state of the art of context-aware recommender systems. The analysis made about the recommenders found in the literature has shown that the ability to combine users' location and movements, together with other aspects like users' preferences, items' properties, or users' ratings, is a complex task that can help to suggest more accurate items. In this sense, we have discovered several open challenges regarding how to reduce well-known problems of recommenders like data sparsity and cold-start. Between these open challenges, we highlight several of them, such as the way of finding similar users when considering their ratings, the way to create users' profiles and classify items, and how to use location and tracking information so as to recommend items. In order to reduce these drawbacks, and following the last goal proposed in this thesis, we proposed a recommender system capable of offering context-aware recommendations and providing automatic ratings, in which the users' movements after receiving recommendations are taken into account (Chapter 3).

III Results

This PhD Thesis is a compilation of a set of publications, so that the results are essentially exposed in the articles that compose it. Following the methodology defined in the previous section to cover the three first objectives of this thesis, we have designed, implemented, and validated a context-aware solution that allows the development of applications by considering the privacy of the users' location. The results derived from the evaluation of the state of the art, as well as the definition and implementation of a context-aware system, have been reported in the IEEE Systems Journal, Special Issue on Intelligent Internet of Things, in a paper entitled "SeCoMan: A Semantic-Aware Policy Framework for Developing Privacy-Preserving and Context-Aware Smart Applications" [25]. In such a paper, we proposed a system that provides support for developing context-aware and smart applications, preserving the users'

privacy in a semantic-oriented vision. Our system is in charge of obtaining the information from the context or environment in which users are located, modeling and protecting their information, and providing context-aware applications. To perform the previous process, we have designed and implemented an architecture oriented to the web semantic techniques [26]. The information about users and contexts is modeled by using a collection of ontologies defined in OWL 2 [27]. The users' information is protected by using policies defined in SWRL [28]. These policies allow users to share their location to the selected users, at the desired granularity, at the right place, and at the right time. Finally, the information about the contexts and users is provided to context-aware applications by using queries defined in SPARQL [29]. In this publication, we included the analysis and comparison of the different context-aware systems. We also included the results regarding the implementation and evaluation of a prototype for a supermarket context, which was chosen due to the amount and richness of the different location-based services that might be potentially provided. A performance analysis showed reasonable times while managing, protecting, and providing information about users and their contexts.

Afterwards, considering the first and second goals, and in order to cover the fourth one defined in this thesis, we investigated further into the protection of the users' information in context-aware solutions. As a result of this research, it was proposed and implemented a platform oriented to protect the users' information regarding services. This result was defined in an article entitled "PRECISE: Privacy-Aware Recommender Based on Context Information for Cloud Service Environments" [30], which was published in IEEE Communications Magazine, Feature Topics Issue on Context-Aware Networking and Communications. In this paper, we defined a privacy-preserving and context-aware system that provides context-aware recommendations by considering the information that users want to reveal to given services. By using our solution, users can release their locations to specific services, hide their positions to specific users, mask their locations to other users by generating fictitious (fake) positions, establish the granularity and closeness at which they want to be located by services or users, and preserve their anonymity to specific services. To perform this, we have designed and deployed an architecture oriented to the MCC paradigm composed of three layers. In our architecture, services are allocated at the Software as a Service (SaaS) layer of the MCC paradigm, providing users with recommendations about context-aware information. The central element of our system is a middleware allocated at the Platform as a Service (PaaS) layer, which preserves the users' information, and manages the information about the context and space that can be provided by independent systems. In this work, we have also included a comparison between the context-aware solutions that can be found in the literature and the main differences with our solution. Among these differences, we highlight the amount of location-aware policies that our solution provides allowing users to have a higher control of their location information.

Finally, the results obtained after covering the fifth and sixth goals of this thesis consist on a context-aware recommender system, which is published in the Journal of Computational Science and it is entitled "Design of a Recommender System Based on Users' Behavior and Collaborative Location and Tracking" [31]. In this paper, we designed a context-aware recommender algorithm with an implicit rating support. Our recommender algorithm combines different approaches in order to rank the suggested items. Specifically, it considers the ratings provided by similar users to the target (Collaborative Filtering approach), the properties of suggested items like price or type (Content Based Filtering approach), and the location and mobility of users and items (Context-Aware approach). Furthermore, our solution provides automatic ratings by taking into account the behavior of the users after receiving recommendations. Aspects like the time and the location of users and items are considered, in order to measure the users' interest for the recommended items and therefore provide ratings according to this information. The management of the information in the recommender is performed by using semantic web

techniques. In this sense, as an extension to our second proposal, we have designed an ontology to model the information of the proposed recommender and rating algorithms. Furthermore, we have analyzed the impact of the aspects considered in the recommender and ratings processes as well as their effectiveness. The results obtained demonstrate improvements on the precision, recall, and F-measure metrics of our proposal, in comparison with others. Furthermore, we have demonstrated that the aspects or parameters considered by our implicit rating algorithm are useful in order to generate implicit (i.e., automatic) ratings.

IV Conclusions and Future Work

The growth of mobile devices has provoked an incredible evolution in information management systems. Nowadays, the majority of these systems are consumed at anytime and anyplace. With this fact, the location of users has become a very valuable information in order to provide services located close to the users. Services using the users' location, in order to provide information about the elements located at the same context, are called context-aware services. The appearance of this kind of services has made more difficult to protect the users' information. Context-aware systems manage valuable information about the users' locations, activities, identities, and other behavior patterns that should be protected. In case that this information is not protected, any user or service provider could obtain this information and misuse it.

Managing and protecting the users' information in context-aware systems based on location is an open issue that still requires efforts to be addressed. Context-aware systems should allow users to control what information they want to reveal, where and when the information will be exchanged, and to whom. Semantic web techniques are a promising way to accomplish the management and protection of contextual and personal information in context-aware systems. This technology allows modeling the information in a formal way, exchanging information between independent systems, defining privacy-policies to protect the information, and inferring new knowledge by considering the information and the policies.

Taking into account the previous facts, in this PhD Thesis has been proposed, analyzed, and implemented a set of solutions to enhance the privacy of the users' information in location-based and context-aware systems. To this end, we have proposed a solution that allows the development of context-aware applications by considering the privacy of the users' location. Our solution called SeCoMan is a trusted middleware that allows users to define their privacy-policies to control where, when, how, and to whom their location information will be revealed to other users. In this sense, users do not have to rely on the context-aware applications, so that our solution is in charge of providing a set of predefined queries that provides information to the context-aware applications. This information is provided by taking into account the privacy-policies defined previously by users in our middleware. In this solution, we have also designed a set of ontologies that model the space and contextual information considered in a supermarket context.

Additionally, we have proposed a context-aware solution oriented to the MCC paradigm, which is in charge of protecting the users' information not only regarding users, but also services. In order to show the usefulness of our solution, we have developed a context-aware recommender capable of providing recommendations to users by considering the information they reveal to the services that provide the recommendations. Using our system, users can control their information by hiding their identities to services, hiding their locations, and providing fake positions, among others.

Finally, our last contribution consists on a context-aware recommender system that combines several approaches, in order to provide effective recommendations and reduce well-known problems of recommender systems like data sparsity and cold-start. In this sense, our solution

combines information provided by the ratings of users similar to the target user, information about the suggested items like the price or type, and information about the context like the distance between users and items or their mobility. On the other hand, we have also proposed a rating algorithm that provides implicit or automatic ratings by taking into account the behavior of users after receiving recommendations. Conducted experiments have provided evidences of the effectiveness of our solution and how the location-based and context-aware parameters used in our recommender and ratings algorithms improve the recommendations.

This PhD Thesis improves some of the drawbacks found in the literature regarding context-aware systems. In this sense, our first contribution was focused on allowing users to control the disclosure of their locations regarding other users by defining privacy-policies. The second proposal of this thesis consists on a context-aware recommender system that allows users to protect other pieces of their sensitive information not only regarding users, but also services. Finally, the last contribution is a context-aware recommendation system in charge of combining several approaches with the users' mobility and location in order to provide enhanced recommendations and automatic ratings.

As a future work, we plan to consider the protection of the privacy of the users' information when users move between several contexts, when there is an exchange of information between them (inter-context scenario). This raises new challenging questions that should be considered like how users would have to manage and protect the information they want to share, who should manage the privacy with respect to the information of the contexts, and what information should be shared between different and independent contexts.

Another future line of work consists on helping users without enough privacy skills in protecting the privacy of their information. In this sense, and depending on the context in which users are located, they will receive several context-aware profiles composed of privacy-policies that protect the users' information in that context.

Publications composing

the PhD Thesis

1

SeCoMan: A semantic-aware policy framework for developing privacy-preserving and context-aware smart applications

Title:	SeCoMan: A Semantic-Aware Policy Framework for Developing Privacy-Preserving and Context-Aware Smart Applications
Authors:	Alberto Huertas Celdrán, Félix J. García Clemente, Manuel Gil Pérez, Gregorio Martínez Pérez.
Journal:	IEEE Systems Journal
Impact factor:	2.114 Q1 (2015)
Publisher:	IEEE
Volume:	10
Number:	3
Pages:	1111-1124
Year:	2016
Month:	September
DOI:	http://dx.doi.org/10.1109/JSYST.2013.2297707
State:	Published

Table 1: SeCoMan: A semantic-aware policy framework for developing privacy-preserving and context-aware smart applications

I Abstract

This paper is intended to provide a solution for developing context-aware smart applications preserving the users' privacy in the Internet of Things (IoT). In this sense, we present a framework called Semantic web-based Context Management (SeCoMan) aimed at offering a set of predefined queries to provide applications with information about indoor location of users and objects, as well as context-aware services. SeCoMan uses a semantic-oriented IoT vision where semantic technologies play a key role. In fact, SeCoMan uses Semantic Web for modeling description of things, reasoning over data to infer new knowledge, and defining context-aware policies. SeCoMan also defines a layered architecture, including functions related to the management of the users' privacy in a manner that accommodate IoT requirements, in addition to not affecting system performance nor introducing excessive overheads. A thorough discussion on other related works, together with some experiments to measure the throughput and scalability, confirm that SeCoMan is a solution that improves the most relevant proposals existing so far.

2

PRECISE: Privacy-aware recommender based on context information for Cloud service environments

Title:	PRECISE: Privacy-aware recommender based on context information for Cloud service environments
Authors:	Alberto Huertas Celdrán, Manuel Gil Pérez, Félix J. García Clemente, Gregorio Martínez Pérez
Journal:	IEEE Communications Magazine
Impact factor:	4.007 Q1
Publisher:	IEEE
Volume:	52
Number:	8
Pages:	90-96
Year:	2014
Month:	August
DOI:	http://dx.doi.org/10.1109/MCOM.2014.6871675
State:	Published

Table 2: PRECISE: Privacy-aware recommender based on context information for Cloud service environments

I Abstract

Context-aware systems based on location open up new possibilities to users in terms of acquiring custom services by gathering context information, especially in systems where the high mobility of users increases their usability. In this context, this article presents a privacy-preserving solution offering context-aware services based on location in MCC. We propose a middleware, called PRECISE, which provides users with custom context-aware recommendations. These recommendations are given by considering the context information, and the users' locations, privacy policies, and previously visited places. MCC plays a key role in this solution, moving the data processing and storage needs to the cloud, as well as further advantages such as elasticity and load balancing. A thorough discussion when comparing PRECISE with other related works confirms that our solution improves the most relevant proposals so far.

3

Design of a recommender system based on users' behavior and collaborative localization and tracking

Title:	Design of a recommender system based on users' behavior and collaborative localization and tracking
Authors:	Alberto Huertas Celdrán, Manuel Gil Pérez, Félix J. García Clemente, Gregorio Martínez Pérez.
Journal:	Journal of Computational Science
Impact factor:	1.078 Q2 (2015)
Publisher:	Elsevier
Volume:	12
Pages:	83-94
Year:	2016
Month:	January
DOI:	http://dx.doi.org/10.1016/j.jocs.2015.11.010
State:	Published

Table 3: Design of a recommender system based on users' behavior and collaborative localization and tracking

I Abstract

During the last years, mobile devices allow incorporating users' location and movements into recommendations to potentially suggest most valuable information. In this context, this paper presents a hybrid recommender algorithm that combines users' location and preferences and the content of the items located close to such users. This algorithm also includes a way of providing implicit ratings considering the users' movements after receiving recommendations, aimed at measuring the users' interest for the recommended items. Conducted experiments measure the effectiveness and the efficiency of our recommender algorithm, as well as the impact of implicit ratings.

Bibliography

[1] B. C. M. Fung, K. Wang, R. Chen, and P. S. Yu. Privacy-preserving data publishing: A survey of recent developments. *ACM Compututer Surveys*, 42(4):14:1–14:53, June 2010.

[2] A. Pingley, W. Yu, N. Zhang, X. Fu, and W. Zhao. CAP: A context-aware privacy protection system for location-based services. In *IEEE International Conference on Distributed Computing Systems*, pages 49–57, June 2009.

[3] H. S. Rekha, C. Prakash, and G. Kavitha. Understanding trust and privacy of big data in social networks - a brief review. In *2014 3rd International Conference on Eco-friendly Computing and Communication Systems*, pages 138–143, December 2014.

[4] P. Yu, X. Ma, J. Cao, and J. Lu. Application mobility in pervasive computing: A survey. *Pervasive and Mobile Computing*, 9(1):2–17, February 2013.

[5] I. A. Junglas and R. T. Watson. Location-based services. *Communications ACM*, 51(3):65–69, March 2008.

[6] M. Weiser. The computer for the 21st century. *Scientific American*, 265(3):94–104, 1991.

[7] G. D. Abowd, A. K. Dey, P. J. Brown, N. Davies, M. Smith, and P. Steggles. Towards a better understanding of context and context-awareness. In *Handheld and Ubiquitous Computing*, pages 304–307, September 1999.

[8] B. Schilit, N. Adams, and R. Want. Context-aware computing applications. In *Proceeding 1st Workshop Mobile Computing Systems and Applications*, pages 85–90, December 1994.

[9] N. Ryan, J. Pascoe, and D. Morse. Enhanced reality fieldwork: The context aware archaeological assistant. In *Proceedings of the 25th Anniversary Computer Applications in Archaeology*, pages 85–90, December 1997.

[10] A. K. Dey. Context-aware computing: The cyberdesk project. In *Proceedings of the AAAI 1998 Spring Symposium on Intelligent Environments*, pages 51–54, 1998.

[11] P. Prekop and M. Burnett. Activities, context and ubiquitous computing. *Computer Communications*, 26(11):1168–1176, July 2003.

[12] R. M. Gustavsen. Condor–an application framework for mobility-based context-aware applications. In *Proceedings of the Workshop on Concepts and Models for Ubiquitous Computing*, volume 39, September 2002.

[13] C. Tadj and G. Ngantchaha. Context handling in a pervasive computing system framework. In *Proceedings of the 3rd International Conference on Mobile Technology, Applications and Systems*, October 2006.

[14] R. Want, A. Hopper, V. Falcão, and J. Gibbons. The active badge location system. *ACM Transactions on Information Systems*, 10(1):91–102, January 1992.

[15] K. R. Wood, T. Richardson, F. Bennett, A. Harter, and A. Hopper. Global teleporting with Java: Toward ubiquitous personalized computing. *Computer*, 30(2):53–59, February 1997.

[16] G. Adomavicius and A. Tuzhilin. Context-aware recommender systems. In *Recommender Systems Handbook*, pages 217–253, September 2011.

[17] F. Ricci, L. Rokach, and B. Shapira. Recommender systems: Introduction and challenges. In *Recommender Systems Handbook*, pages 1–34, 2015.

[18] K. Verbert, N. Manouselis, X. Ochoa, M. Wolpers, H. Drachsler, I. Bosnic, and E. Duval. Context-aware recommender systems for learning: A survey and future challenges. *IEEE Transactions on Learning Technologies*, 5(4):318–335, October 2012.

[19] R. Hull, B. Kumar, D. Lieuwen, P. F. Patel-Schneider, A. Sahuguet, S. Varadarajan, and A. Vyas. Enabling context-aware and privacy-conscious user data sharing. In *IEEE International Conference on Mobile Data Management*, pages 187–198, January 2004.

[20] O. Yurur, C. H. Liu, Z. Sheng, V. C. M. Leung, W. Moreno, and K. K. Leung. Context-awareness for mobile sensing: A survey and future directions. *IEEE Communications Surveys Tutorials*, 18(1):68–93, Firstquarter 2016.

[21] F. L. Gandon and N. M. Sadeh. Semantic web technologies to reconcile privacy and context awareness. *Web Semantics: Science, Services and Agents on the World Wide Web*, 1(3):241–260, April 2004.

[22] I. Horrocks. Ontologies and the semantic web. *Communications ACM*, 51(12):58–67, December 2008.

[23] J. Bernal Bernabé, G. Martínez Pérez, and Antonio F. Skarmeta Gómez. Intercloud trust and security decision support system: An ontology-based approach. *Journal of Grid Computing*, 13(3):425–456, September 2015.

[24] K. Kravari, N. Bassiliades, and G. Governatori. A policy-based B2C e-Contract management workflow methodology using semantic web agents. *Artificial Intelligence and Law*, 24(2):93–131, June 2016.

[25] A. Huertas Celdrán, F. J. García Clemente, M. Gil Pérez, and G. Martínez Pérez. SeCoMan: A semantic-aware policy framework for developing privacy-preserving and context-aware smart applications. *IEEE Systems Journal*, 10(3):1111–1124, September 2016.

[26] T. Berners-Lee, J. Hendler, and O. Lassila. The semantic web. *Scientific American*, 284(5):28–37, May 2001.

[27] B. Motik, P. F. Patel-Schneider, and B. Parsia (ed.). OWL 2 web ontology language: Structural specification and functional-style syntax. *W3C Recommendation*, September 2012.

[28] I. Horrocks, P. F. Patel-Schneider, H. Boley, S. Tabet, B. Grosof, and M. Dean. SWRL: A semantic web rule language combining OWL and RuleML. *W3C Member submission*, 21:79, May 2004.

[29] E. Prud'hommeaux and A. Seaborne. SPARQL query language for RDF. *W3C Recommendation*, January 2008.

[30] A. Huertas Celdrán, M. Gil Pérez, F. J. García Clemente, and G. Martínez Pérez. PRECISE: Privacy-aware recommender based on context information for cloud service environments. *IEEE Communications Magazine*, 52(8):90–96, August 2014.

[31] A. Huertas Celdrán, M. Gil Pérez, F. J. García Clemente, and G. Martínez Pérez. Design of a recommender system based on users' behavior and collaborative location and tracking. *Journal of Computational Science*, 12:83–94, January 2016.