UNIVERSIDAD DE MURCIA

FACULTAD DE INFORMÁTICA

Authorization and Trust Management in Distributed Systems
Based on the Semantic Web

Gestión de la Autorización y la Confianza en Sistemas Distribuidos
Aplicando la Web Semántica

D. Jorge Bernal Bernabé
2015

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

1. Jorge Bernal Bernabé, Juan Manuel Marín Pérez, Jose M. Alcaraz Calero, Félix J. García Clemente, Gregorio Martínez Pérez, Antonio F. Gómez Skarmeta. "Towards an Authorization System for Cloud Infrastructure Providers", SECRYPT 2011 - Proceedings of the International Conference on Security and Cryptography, pp. 333 - 338, ISBN: 978-989-8425-71-3, July 2011, http://dx.doi.org/10.5220/0003525703330338

2. Juan Manuel Marín Pérez, Jorge Bernal Bernabé, Jose M. Alcaraz Calero, Félix J. García Clemente, Gregorio Martínez Pérez, Antonio F. Gómez Skarmeta. "Taxonomy of trust relationships in authorization domains for cloud computing", The Journal of Supercomputing, Springer, Vol 70, pp 1075-1099, December 2014. http://dx.doi.org/10.1007/s11227-014-1117-x

3. Jorge Bernal Bernabé, Gregorio Martínez Pérez, Antonio F. Skarmeta Gómez. "Intercloud Trust and Security Decision Support System: an Ontology-based approach", Journal of Grid Computing, September 2015, Published Online. http://dx.doi.org/10.1007/s10723-015-9346-7

4. Jorge Bernal Bernabé, Jose Luis Hernańdez Ramos and Antonio F. Skarmeta Gómez . "TACIoT: multidimensional trust-aware access control system for the Internet of Things", Soft Computing, Springer, May 2015, Published Online. http://dx.doi.org/10.1007/s00500-015-1705-6

Table of Contents

Agradecimientos/Acknowledgements

Agradecimientos

En primer lugar me gustaría dar las gracias a mi familia. A mis padres, Encarna y Bartolo, fuente de apoyo constante e incondicional, por haberme dado el cariño y la educación que me han hecho llegar hasta aquí. Por su paciencia, por los valores que me han transmitido, y por ser un constante ejemplo a seguir. Sin vuestra ayuda, nada hubiera sido posible. A mis hermanas Bea y María José, porque siempre han estado a mi lado en los momentos difíciles, demostrado lo mucho que me quieren. A toda mi familia, tíos, primos, abuelos y sobrinos, en especial a mi Tati y mi abuelo Pepe Panú por todo su cariño, mil gracias.

Quiero expresar mi más grande agradecimiento a Sensi por todo su amor, apoyo y comprensión. Gracias por darle sentido a mi vida y traer al mundo a este hijo tan maravilloso que tenemos y que se ha convertido en la razón de mi existencia. Jorge eres mi orgullo y mi gran motivación, libras mi mente de todas las adversidades que se presentan, impulsándome a diario a superarme para ofreceros lo mejor.

A todos y cada uno de los amigos que me han acompañado a lo largo de mi vida en diferentes ámbitos. A mis compañeros del colegio, del instituto, de los scouts, de judo, de la banda de música, del carnaval, de la universidad,..., a todos gracias por los momentos vividos. Como olvidar igualmente a cada uno de los profesores que han puesto su granito de arena en mi educación, gracias.

A mis directores de tesis, Gregorio y Antonio, por haberme dado esta oportunidad y haber confiado en mí desde el principio. Gracias por vuestro apoyo, por enseñarme tantas cosas e inculcarme valores de mejora continua, perseverancia y superación, sin vosotros esto nunca habría sido posible, gracias.

Por último me gustaría dar las gracias a todos mis compañeros del trabajo, y en especial a José María y Juan-Ma, mis amigos y compañeros de fatigas, gracias por hacer que esta tesis sea hoy sea una realidad, gracias por apoyarme y ayudarme, gracias por hacer que trabajar con vosotros sea un verdadero placer.

Acknowledgements

First I would like to thank my family. My parents, Encarna and Bartolo, source of constant and unconditional support, for giving me the love and education that have made me get here. For your patience, for the values that you have given to me, and for being a constant role model. Without your help, nothing would have been possible. My sisters Bea and Maria Jose, because they have always been there for me in difficult moments, showing how much they love me. To all my family, uncles, cousins, grandparents and nephews, especially my Tati and my grandfather Pepe Panú for all their love, thank you.

I want to express my greatest gratitude to Sensi for all your love, support and understanding. Thank you for giving meaning to my life and give birth to this wonderful child that we have and who has become the reason for my existence. Jorge you are my pride and great motivation, making me freeing my mind from all the adversities that are presented daily, encouraging me to improve myself in order to offer you the best.

For each of the friends who have gone along with me throughout my life in different areas. My classmates in school, in high school, scouts, judo, orchestra, carnival, university colleges ... thanks for all the moments. I couldn't also forget every teacher who have put their two cents in my education, thanks.

My thesis supervisors, Gregorio and Antonio, for giving me this opportunity and have trusted me from the beginning. Thanks for your support, for teaching me so many things and instil values of continuous improvement, perseverance and overcoming, without you this would have been never possible, thanks.

Finally, I would like to thank all my co-workers, and especially to José Maria and JuanMa, my friends and fellow sufferers, thanks for making this thesis a reality, thanks for supporting me and helping me, thanks for making working with you to be a real pleasure.

Resumen

I Motivación y Objetivos

Las tecnologías de la información y las comunicaciones (TIC) evolucionan constantemente con el fin de satisfacer las nuevas demandas de la sociedad. Esta tendencia está llevando a los sistemas distribuidos de computadoras a una nueva era donde las infraestructuras de dichos sistemas requieren capacidades dinámicas de escalabilidad con el fin de proporcionar servicios bajo demanda y en el momento oportuno. El emergente paradigma de Cloud Computing [10] satisface estos aspectos suministrando arquitecturas TIC virtuales, donde los recursos gestionados se crean y desmantelan dinamicamente, atendiendo a las necesidades variables de los usuarios. Cloud Computing proporciona algunas características clave como la provisión de servicios bajo demanda, el acceso ubicuo, la elasticidad y el pooling de recursos.

Además, cualquier sistema distribuido como Cloud Computing se enfrenta a diferentes retos de seguridad, como son la autenticación, autorización, privacidad o la gestión de la confianza [113]. Sin embargo, aunque existen algunas propuestas e implementaciones iniciales para gestionar los aspectos de seguridad en Cloud Computing, se precisan sistemas de autorización y confianza avanzados y con altos niveles de expresividad que hayan sido diseñados expresamente para Cloud Computing, donde las características propias de la arquitectura, como son el multi-tenancy [90], introducen nuevos riesgos de seguridad y por lo tanto nuevas necesidades de autorización. Los sistemas de autorización y confianza desplegados actualmente en Cloud Computing han sido heredados de diseños previos para otras arquitecturas, y por lo tanto, no han sido del todo adaptados para funcionar en estos nuevos escenarios.

La gestión de la seguridad en sistemas distribuidos como Cloud Computing puede llevarse a cabo, entre otras aproximaciones, mediante el uso de políticas y reglas de seguridad aplicadas sobre modelos de sistema y seguridad enriquecidos semánticamente. El enfoque de la Web Semántica [22] permite realizar razonamiento deductivo y procesos de inferencia sobre los modelos, permitiendo deducir conclusiones de seguridad que a su vez pueden ser usadas para tomar decisiones de autorización y confianza, adaptando el sistema para que reaccione en base a tales conclusiones.

En este sentido, la Web Semántica puede ser empleada como elemento principal de un sistema de autorización altamente expresivo semánticamente, habilitando de esta forma características avanzadas y novedosas de autorización que no han sido del todo tratadas conjuntamente en Cloud Computing. Un sistema de control de acceso avanzado podría aprovechar los formalismos lógicos proporcionados por las tecnologías de la Web Semántica para describir los modelos de autorización y de sistema, así como para hacer uso de reglas semánticas que protejan el acceso de los recursos en el cloud.

El sistema de autorización es crucial para gestionar el acceso de los recursos en el cloud por parte de los diferentes *tenants*. No obstante, además de la gestión de la autorización de los recursos de forma independiente por cada tenant, los clientes en el mismo cloud pueden necesitar colaborar entre ellos para satisfacer necesidades avanzadas de sus servicios, lo que requiere de modelos de autorización y confianza intra-cloud para gestionar tales colaboraciones. Por ejemplo, supongamos que dos organizaciones que ofrecen sus servicios en el cloud quieran alcanzar acuerdos para ofrecer un servicio común que a su vez haga uso de sus servicios actuales. Ambos tenants del mismo cloud, usan sus recursos computacionales para ofrecer su parte del servicio común. En el caso de que en un momento dado un tenant no disponga de los recursos suficientes (ya sea computacionales, de red o almacenamiento) para satisfacer la demanda de sus servicios, podría utilizar los recursos del otro tenant para escalar y poder continuar proporcionando el servicio común. De esta forma las organizaciones podrían sacar ventaja de estos tipos de alianzas para compartir recursos y evitar tener que alquilar más recursos del cloud.

Sin embargo estos tipos de relaciones de alianza entre los tenants no está soportada en los clouds actuales. La pila de Cloud Computing debería soportar esta característica permitiendo los acuerdos colaborativos entre los clientes que comparten los recursos en el mismo cloud. No obstante, estas relaciones de confianza conllevan nuevos riesgos de seguridad, ya que las entidades participantes deben confiar entre ellas para poder compartir los recursos y servicios. Las entidades pueden cooperar a diferentes niveles de confianza, en función de su disposición a compartir recursos. Creemos que estos tipos de colaboraciones no han sido estudiados y analizados lo suficiente y que, por lo tanto, hay diferentes nichos de investigación en este sentido.

Por otro lado, la barrera tecnológica derivada de la dependencia de los usuarios a un software de cloud determinado complica sobremanera las interacciones entre diferentes clouds para realizar operaciones tales como migraciones de datos y servicios. Esta situación lleva a la necesidad de diseñar nuevas soluciones para permitir a los proveedores de servicios de cloud (CSPs) que puedan interactuar de forma segura estableciendo federaciones de clouds, paradigma conocido como Intercloud [23]. Este entorno pretende capacitar a los usuarios y proveedores con herramientas para interactuar con varios clouds de forma segura, así como comparar los servicios ofrecidos por estos, su precio, calidad de servicio y características de seguridad con el fin de seleccionar el más efectivo. Al mismo tiempo los CSPs están empezando a requerir el establecimiento de colaboraciones dinámicas para absorber picos de demanda en cuanto a computación, almacenamiento y redes. Desde el punto de vista de los CSPs, el establecimiento de colaboraciones cloud dinámicas les permite gestionar de forma eficiente los recursos del cloud consiguiendo economías de escala e incrementando las capacidades de servicio.

El paradigma de Intercloud se encuentra todavía en sus primeras etapas y, por lo tanto, lleno de oportunidades de investigación [44]. Entre ellos cabe destacar portabilidad, interoperabilidad, modelado, migración, soporte de infraestructura, monitorización, testing, despliegue de aplicaciones, normas y regulaciones legales, SLAs, protección de datos, privacidad y seguridad. Aunque actualmente existen algunas investigaciones iniciales sobre la gestión de Intercloud, dichas propuestas se centran en aspectos de interoperabilidad en cuanto a interfaces y modelos de datos a nivel de la capa de infraestructura (IaaS), y no tanto en cuanto a retos de seguridad, privacidad y confianza. Por lo tanto se requieren nuevas propuestas que permitan a diferentes clouds interactuar de forma segura con el fin de proporcionar un entorno Intercloud heterogéneo y a la vez confiable.

Entre los retos de seguridad en el Intercloud, el análisis de la seguridad y la confianza que puede llegar a ofrecer un proveedor de servicios de cloud es un campo de investigación que despierta un elevado interés. A pesar de que existen otros modelos para cuantificar la confianza de un CSP o servicio, dichos modelos no tienen en cuenta realmente un amplio abanico de aspectos de seguridad y, además, no basan la cuantificación en evaluaciones reales de seguridad realizadas sobre el servicio o el CSP, sino más bien, en interacciones pasadas y opiniones de terceros.

Las evaluaciones de seguridad pueden ser intercambiadas en el Intercloud para hacerlo más seguro. En este sentido, las tecnologías de la Web Semántica pueden ser empleadas como mecanismo para intercambiar información de seguridad sobre un determinado CSP. El uso de ontologías, a diferencia de otros modos de expresar taxonomías y modelos, otorga un alto nivel de interoperabilidad semántico entre los CSPs. Sin embargo, actualmente no existen ontologías de seguridad especialmente diseñadas para el Intercloud.

Al mismo tiempo, los clientes y CSPs podrían beneficiarse de un sistema de ayuda a la decisión relativo a seguridad y confianza en entornos Intercloud. Este sistema podría deducir información y tomar decisiones en consecuencia, tales como rechazar o evitar determinadas interacciones entre CSPs o servicios. No obstante, las soluciones de Intercloud actuales no soportan este tipo de sistemas de ayuda a la decisión. Concretamente, el sistema podría estar basado en la ontología de seguridad mencionada anteriormente para habilitar la aplicación de técnicas de la Web Semántica que ayuden en el proceso de ayuda a la decisión de seguridad, y de este modo, determinar si un determinado CSP puede ser confiable en un contexto determinado.

Cloud Computing está siendo aplicado en diferentes escenarios para mejorar sustancialmente las posibilidades de los mismos. Entre los escenarios con más posibilidades de expansión se encuentran aquellos derivados de la aplicación del paradigma del Internet de las Cosas [11] (IoT por sus siglas en inglés). Bajo la visión de IoT, millones de dispositivos interconectados, y sus servicios derivados, generan datos masivos que son procesados y analizados con diferentes propósitos, como por ejemplo la identificación de patrones dentro de dichos datos. El éxito de los servicios de IoT se alcanza únicamente si tales servicios pueden ser accedidos ubicuamente, eficientemente, de forma segura y confiable (tratando los cambios de políticas/contexto y gestionando la confianza entre los servicios y entidades), con un alto nivel de rendimiento, y de forma escalable (ya que pueden necesitarse una gran cantidad dinámica de recursos y datos masivos para proporcionar los servicios IoT). Las características que ofrece Cloud Computing, mencionadas al principio de esta sección, cumplen con estos requisitos y son por tanto, hoy día esenciales para proporcionar los servicios del mundo IoT.

En IoT dispositivos heterogéneos están continuamente intercambiando información y siendo accedidos ubicuamente a través de redes dadas a pérdida, con protocolos no orientados a la conexión. Los escenarios IoT requieren de modelos adaptados para la gestión y cuantificación de la confianza con el fin de que dispositivos desconocidos a priori puedan interactuar entre ellos de forma segura y confiable. Además, los sistemas de control de acceso tradicionales no encajan correctamente en entornos IoT, donde se tienen que gestionar no sólo comunicaciones centralizadas sino también comunicaciones máquina a máquina (M2M). Los modelos de control de acceso en IoT deben ser más livianos para poder tratar las comunicaciones directas entre dispositivos (a veces con características hardware reducidas), y tener en cuenta los valores de confianza de los dispositivos antes de realizar las transacciones. Asimismo, los modelos de cuantificación de confianza en IoT deberían tener en cuenta diferentes factores, más allá de la reputación, para calcular los valores de confianza. En este sentido, en el estado de arte actual hay una carencia de sistemas avanzados diseñados para IoT que permitan, entre otras características, la cuantificación de la confianza teniendo en cuenta un conjunto extenso de consideraciones para calcular un valor de confianza de los dispositivos.

Dados los retos de investigación relativos a gestión de la confianza y la autorización en sistemas distribuidos destacados anteriormente, los principales propósitos de la presente tesis doctoral pueden ser resumidos en dos grandes objetivos. Por una parte, el principal objetivo es hacer Cloud Computing más confiable mediante el diseño y la implementación de modelos de autorización y confianza avanzados que se apoyen en tecnologías de la Web Semántica. Por otra parte, el segundo objetivo es proporcionar un modelo de confianza enfocado a escenarios más descentralizados, como los derivados del Internet de las Cosas, mejorando además los mecanismos actuales de control de acceso para que puedan tener en cuenta la confianza calculada por el modelo.

De esta forma los objetivos concretos perseguidos en esta tesis, derivados de los dos objetivos generales descritos anteriormente, son los siguientes:

- Analizar y diseñar un modelo de autorización, altamente expresivo, diseñado especialmente para Cloud Computing que se apoye en técnicas de la Web Semántica.
- Analizar y diseñar las diferentes relaciones de confianza que puedan establecerse en Cloud Computing entre los diferentes tenants, incrementando de esta forma la seguridad del cloud.
- Analizar el estado del arte relativo a seguridad y confianza en sistemas distribuidos, Cloud Computing y especialmente en Intercloud.
- Analizar los requerimientos de seguridad en Cloud Computing definiendo en consecuencia una taxonomía y ontología completas para el Intercloud.
- Diseñar, implementar y validar un sistema de ayuda a la decisión relativo a seguridad y confianza que se apoye en técnicas de la Web Semántica con el fin de mejorar la toma de decisiones, cuantificando expectativas de seguridad e índices de confianza sobre CSPs.
- Diseñar, implementar y validar un modelo de confianza para el Internet de las Cosas (IoT), que pueda ser aplicado junto a un sistema de autorización que tenga en cuenta los índices de confianza calculados por el modelo.

II Metodología

La presente tesis doctoral vio sus comienzos con un estudio del estado del arte en gestión de la seguridad para sistemas distribuidos. Por aquel entonces ya éramos conscientes que una aproximación de gestión basada en políticas era una potente herramienta para administrar la seguridad de sistemas de computación complejos. Bajo este modelo de administración, los sistemas distribuidos pueden ser gestionados de forma eficiente manteniendo un orden, seguridad y consistencia apropiados. Al mismo tiempo, el paradigma de la Web Semántica había evolucionado lo suficiente como para ser utilizado como mecanismo para enriquecer semánticamente tanto modelos de sistema como las políticas de seguridad, lo que nos permitiría incrementar notablemente las posibilidades de los sistemas basados en políticas. De esta forma comenzamos a investigar sobre el uso de técnicas de la Web Semántica para la gestión de la seguridad en sistemas distribuidos. Esto nos llevó a empezar a definir modelos semánticos de sistemas de información y de seguridad con el fin de realizar razonamiento sobre dichos modelos usando políticas enriquecidas semánticamente.

Concretamente, durante el análisis del estado del arte descubrimos que había una carencia de modelos de autorización altamente expresivos haciendo uso de la Web Semántica que pudieran gestionar de forma adecuada la complejidad de sistemas distribuidos como Cloud Computing. Los modelos de autorización actuales para Cloud Computing, aunque eficientes, están condicionados debido a sus limitadas posibilidades de expresividad semántica y, como consecuencia, limitados en cuanto a capacidades de autorización. Así, entre el diverso número de tópicos de investigación de seguridad para sistemas distribuidos nos centramos en el nicho de investigación referente a la autorización utilizando sistemas basados en políticas basados en la Web Semántica.

Después del estudio de aplicabilidad de las técnicas de la Web Semántica para autorización en Cloud Computing, propusimos un modelo de autorización para hacer frente a este reto (Capítulo 1). Dicho modelo de autorización, a diferencia de modelos de autorización previos, está basando en la Web Semántica, por lo que permite realizar razonamiento e inferencia sobre los modelos ontológicos y las políticas, otorgando un mecanismo muy potente para tomar decisiones de control de acceso. Este mecanismo permite tratar con garantías diversas características avanzadas de autorización. Entre estas características cabe mencionar el control de acceso basado en roles (RBAC por sus siglas en inglés), RBAC jerárquico (hRBAC), RBAC condicional (cRBAC) y objetos jerárquicos (HO).

Durante la investigación realizada para concebir el modelo de autorización, descubrimos que no existían estudios y modelos formales que definieran las relaciones de confianza que pueden establecerse entre los tenants de un mismo cloud. Los tenants deberían poder establecer alianzas y coaliciones federadas para sacar máximo partido de sus servicios. Este escenario ocasiona diferentes problemas y retos de seguridad como la gestión del control de acceso intra-cloud. Los tenants deberían disponer de medios para restringir y definir qué información estará disponible para con otros tenants que compartan la misma infraestructura cloud subyacente. Este problema de compartición de infrastructura está derivado de la condición de multi-tenancy presente en Cloud Computing. Sin embargo, las soluciones cloud actuales no permiten la definición de este tipo de colaboraciones, y no existe ningún estudio formal de los tipos de relaciones de confianza entre tenants y sus implicaciones de seguridad y privacidad.

Para llenar este vacío, realizamos un análisis y estudio de los tipos de colaboraciones, que consideramos más importantes, y que podrían llegar a ocurrir entre los tenants de un mismo cloud, que dio como resultado una taxonomía que define los diferentes tipos de relaciones de confianza entre tenants (Capítulo 2). La taxonomía de relaciones de confianza tiene en cuenta aspectos de privacidad, riesgo asumido, así como la facilidad a la hora de definir y administrar los acuerdos de confianza. Las relaciones de confianza son, posteriormente, desplegadas e implementadas mediante la aplicación de un modelo de autorización adecuado que pueda tener en cuenta tales relaciones de confianza.

Asimismo, además de las relaciones intra-cloud entre tenants, los clientes y proveedores de cloud están empezando a requerir escenarios incipientes de Intercloud, donde diferentes clouds interaccionan más allá de un único proveedor. Aunque existen algunos resultados de investigación para gestión de Intercloud, hay muy pocas propuestas relacionadas con la seguridad y los aspectos de confidencialidad en el Intercloud. Con el fin de llenar este vacío, realizamos un estudio riguroso del estado del arte en el Intercloud, analizando los aspectos de seguridad y confianza en este entorno distribuido. Como resultado obtuvimos una ontología destinada a definir formalmente los aspectos de seguridad que pueden ser susceptibles de ser modelados en una evaluación de seguridad Intercloud (Capítulo 3). La ontología está basada en estándares de seguridad actuales, se apoya en una ontología existente llamada mOSAIC[91] y ha sido diseñada para hacer frente a los requisitos de seguridad de los diferentes escenarios Intercloud.

Además, la ontología es usada por un novedoso sistema de ayuda a la decisión sobre aspectos de seguridad y confianza en el Intercloud llamando Trust-DSS, acrónimo en Ingles de "Trust and Security Decision Support System". Nuestro sistema Trust-DSS permite ayudar en la toma de decisiones de seguridad, cuantificando expectativas de seguridad y confianza sobre proveedores de servicios del cloud (CSPs). Puesto que el sistema Trust-DSS se basa en la Web Semántica, es capaz de realizar inferencia sobre la ontología de seguridad y reglas semánticas para detectar situaciones anómalas de seguridad y conflictos presentes en las evaluaciones. Al final, permite desestimar o evitar la interacción con ciertos CSPs o servicios en el cloud basándose en estas deducciones.

Por último, hemos querido abordar el control de acceso y gestión de la confianza no sólo en los sistemas distribuidos más centrados en plataforma como Cloud Computing, sino también en otros escenarios más descentralizados. En este sentido, el paradigma emergente de Internet de las Cosas (IoT), se caracteriza por sus redes con pérdidas y comunicaciones máquina a máquina (M2M) que requieren la adaptación de modelos de confianza y autorización actuales. El enfoque tradicional y centralizado requiere de una intervención continua de una entidad central llamada PDP (Policy Decision Point) encargada de tomar decisiones de autorización, lo cual es un inconveniente para algunos escenarios IoT. De esta manera, realizamos un análisis del estado del arte de los modelos de confianza para la IoT, así como modelos de autorización que pudieran tener en cuenta los índices de confianza en escenarios M2M. El objetivo era mejorar la fiabilidad en los escenarios IoT, donde los dispositivos inicialmente desconocidos son propensos a interactuar entre sí. Como resultado de este análisis, descubrimos que no había ningún modelo de confianza especialmente ideado para los escenarios de la IoT que pudiera desplegarse junto con un modelo de autorización también diseñado para IoT. Por lo tanto, hemos diseñado un mecanismo de seguridad, aprovechando un sistema de autorización IoT ya existente llamado DCapBAC [60], que mejora dicho sistema de autorización para que tenga en cuenta valores de confianza calculados por un modelo de confianza que considera no sólo la reputación, que ya se emplea comúnmente en redes entre pares (P2P, por sus siglas en inglés), sino también otros aspectos avanzados para cuantificar la confianza (Capítulo 4).

III Resultados

Esta tesis doctoral fue concebida desde el principio como una tesis por compendio de publicaciones, por lo que los resultados se exponen fundamentalmente en los artículos que la forman. Los primeros resultados derivados del análisis y diseño de un sistema de control de acceso para Cloud Computing se presentaron en "International Conference on Security and Cryptography" (SECRYPT), en un artículo titulado "Towards an Authorization System for Cloud Infrastructure Providers" [19] . En dicho artículo presentamos el sistema de autorización de Cloud Computing que aborda el asunto de multi-tenancy en Cloud Computing. La propuesta se basa en las tecnologías de la Web Semántica, haciendo uso de reglas semánticas SWRL[61] para gestionar el comportamiento del modelo, así como de la definición de modelo del sistema que se representa en forma ontólogica en OWL[54], que ha sido derivado del estándar Common Information Model (CIM) [28]. En el artículo dejamos patente que las tecnologías de la Web Semántica ofrecen herramientas muy útiles para describir modelos de autorización adecuados en entornos distribuidos. Dicha aproximación permite inferir nuevos conocimientos que permiten soportar diferentes características avanzadas de autorización, superando ciertas carencias de expresividad de modelos de autorización predecesores, como el RBAC, hRBAC, cRBAC y HO.

Seguidamente realizamos una investigación minuciosa de los diferentes tipos de relaciones de confianza que pueden establecerse entre tenants en el cloud. El resultado quedó reflejado en el artículo "Taxonomy of trust relationships in authorization domains for Cloud Computing" [85], que fue publicado en la revista The Journal of Supercomputing. El análisis realizado concluyó con la descripción formal de las diferentes relaciones de confianza en Cloud Computing. Dichas relaciones permiten la definición de diferentes acuerdos de colaboración en diferentes escenarios cloud. Además, este trabajo presenta una comparación de los diferentes tipos de relaciones de confianza, analizando aspectos como el control de la privacidad, el riesgo asumido, el nivel de confianza y la facilidad de gestión. El trabajo incluye además el diseño de una arquitectura de gestión de la confianza que permite a los tenants hacer uso de las definiciones de relaciones de confianza con el fin de gestionar y controlar los acuerdos de colaboración entre ellos. La arquitectura ha sido validada por medio de un prototipo implementado con el uso de las tecnologías de la Web Semántica. Asismismo, el artículo también presenta un conjunto diverso de escenarios comunes en Cloud Computing, proponiendo las relaciones de confianza que se consideran más convenientes para cada caso.

Los resultados de investigación relativos a modelos de confianza y seguridad en el Intercloud se muestra en el artículo "Intercloud Trust and Security Decision Support System: an Ontology-based approach" [68], que se encuentra actualmente aceptado y en fase de publicación en la revista Journal of Grid Computing. En este trabajo hemos analizado las diferentes áreas de seguridad, propiedades y métricas que pueden ser necesarias en la evaluación de la seguridad de un CSP. Estos conceptos se han modelado en la ontología SOFIC [121] ofreciendo un alto grado de interoperabilidad en escenarios Intercloud. La ontología se puede tomar como punto de partida para cuantificar expectativas de seguridad y valores de confianza de servicios y CSPs, proporcionando un instrumento muy interesante para los usuarios ya que les sirve de ayuda en el proceso de toma de decisiones de seguridad en el Intercloud. SOFIC está accesible públicamente, se basa en estándares y ha sido ideada de forma extensible y adaptable con el fin de hacer frente a los requisitos de seguridad de los diferentes escenarios Intercloud.

La investigación en el Intercloud ha demostrado las ventajas de disponer de una ontología OWL para modelar aspectos de seguridad de Cloud Computing. El artículo recoge una serie de experimentos realizados con el fin de validar el rendimiento y viabilidad del sistema de ayuda a la decisión relativo a confianza y seguridad (Trust-DSS). En este sentido, nuestro sistema es capaz de manejar adecuadamente y de forma simultánea una cantidad apropiada de evaluaciones históricas sobre los CSP. Además, muestra cómo puede llevarse a cabo de manera eficiente un proceso de evaluación de la confianza y ayuda a la toma de decisiones de seguridad utilizando tecnologías de la Web Semántica. Este mecanismo proporciona un instrumento útil para comprobar determinadas restricciones de seguridad y detectar conflictos presentes en las evaluaciones, lo que permite, entre otras cosas, evitar interacciones con ciertos CSP o servicios en el cloud que puedan ser poco fiables. El artículo pone de manifiesto la capacidad de nuestra propuesta para deducir valores de expectativas de seguridad acerca de diferentes propiedades evaluadas. Asimismo, el sistema de ayuda a la decisión Trust-DSS proporciona un modelo para el cálculo de índices de confianza de manera eficiente, basándose en un modelo que combina la aritmética y técnicas de lógica difusa y que considera evaluaciones históricas y otros parámetros que permiten personalizar el modelo.

Por último, en relación con el modelo de confianza para el Internet de las Cosas, nuestros resultados de investigación han sido publicados en la revista Soft Computing, en un artículo con el título "TACIoT: multidimensional trust-aware access control system for the Internet of Things" [21]. El artículo proporciona un modelo de confianza para IoT y mejora el sistema de control de acceso DCapBAC para que pueda tener en cuenta los valores de confianza calculados por el modelo, y por lo tanto, que pueda tomar decisiones de autorización en consecuencia. El modelo de confianza está especialmente diseñado para la IoT, teniendo en cuenta cuatro dimensiones para calcular los valores de confianza de los dispositivos: calidad de servicio, reputación, aspectos de seguridad y relaciones sociales. El modelo TACIoT ha sido implementado haciendo uso de un sistema de control difuso, que se basa en las cuatro dimensiones de confianza, que a su vez, se cuantifican a partir de históricos de propiedades y evidencias. Los experimentos realizados demuestran la viabilidad de la investigación cuando ha sido llevada a escenarios reales de IoT, tanto en despliegues en dispositivos restringidos como no restringidos. Los resultados obtenidos muestran tiempos interesantes para ambos tipos de dispositivos cuando se realiza el proceso de control de acceso teniendo en cuenta dichos valores de confianza.

IV Conclusiones y Trabajo Futuro

Cloud Computing está evolucionando rápidamente para satisfacer las nuevas demandas de la sociedad. Sin embargo, las nuevas oportunidades que ofrece este nuevo paradigma llevan asociadas diversos riesgos de seguridad. Aunque las soluciones de seguridad tradicionales con respecto a la autorización y gestión de la confianza han demostrado ser bastante eficaces en los escenarios anteriores, la constante evolución del cloud junto con sus nuevas necesidades de seguridad las hacen no del todo adecuadas para escenarios de Cloud Computing e InterCloud.

El establecimiento de un entorno cloud confiable es un tema de investigación incipiente que aún requiere de un esfuerzo de colaboración común para que pueda implantarse con éxito y con suficientes garantías. Las particularidades de Cloud Computing como el multi-tenancy y la virtualización, plantean nuevos problemas de seguridad que requieren de nuevos mecanismos actualizados para aumentar la fiabilidad, la seguridad y la confianza en este entorno distribuido. En este sentido, Cloud Computing requiere modelos más expresivos de autorización a fin de superar ciertas carencias de los principales modelos actuales. Además, dotar al Cloud Computing con capacidades de federación y definición de las relaciones de confianza entre los clientes es un tema de investigación abierto no tratado todavía en el estado del arte. Asimismo, los modelos de confianza actuales para el Intercloud no se basan en evaluaciones de seguridad sobre los proveedores de servicios cloud, que ofrecen una poderosa herramienta para evaluar los CSP y tomar decisiones de seguridad en consecuencia.

Esta tesis doctoral ha propuesto un conjunto de soluciones con el fin de mejorar la confianza digital en Cloud Computing y superar los nichos de investigación mencionadas anteriormente. En primer lugar, hemos propuesto un sistema de control de acceso semántico que soporta una alta expresividad en la definición de políticas y modelos con el fin de soportar funciones avanzadas de autorización.

Para hacer frente a los acuerdos de colaboración intra-cloud establecidos hemos propuesto una descripción formal de los diferentes tipos de relaciones de confianza que pueden ocurrir en diferentes escenarios. Esto ha dado lugar a un interesante análisis y taxonomía, con una comparativa de los diferentes tipos de relaciones de confianza y su adecuación a los escenarios comunes en Cloud Computing, teniendo en cuenta diferentes aspectos clave como el control de la privacidad, el riesgo asumido, el nivel de confianza y facilidad de gestión.

Asimismo, hemos propuesto un sistema de ayuda a la decisión sobre aspectos de confianza y seguridad (Trust-DSS) para el Intercloud, junto con una ontología de seguridad llamada SOFIC. Creemos que el resultado es una herramienta interesante para los clientes del cloud, ya que los dota de mecanismos para resolver dinámicamente las expectativas de seguridad y confiabilidad de un CSP dado. El sistema les dota de información valiosa para adecuar su comportamiento en el cloud de acuerdo con las conclusiones inferidas, aumentando su seguridad y confianza en los sistemas cloud.

Por otra parte, los modelos de confianza para el IoT pueden cuantificar índices de confianza mediante la recopilación de diferentes tipos de información provenientes de diferentes fuentes. Los dispositivos pueden generar su propia opinión sobre cómo de confiable es otro dispositivo cuando se realiza una acción específica en un contexto dado. Los valores de confianza se pueden tener en cuenta en el momento de la toma de decisión de autorización, lo que reduce posibles amenazas y riesgos de seguridad. En este sentido, esta tesis ha propuesto y evaluado satisfactoriamente un modelo de confianza avanzado especialmente diseñado para la IoT que sigue un enfoque multidimensional para calcular los valores de confianza de los dispositivos. El modelo tiene en cuenta no sólo la reputación obtenida de terceras entidades, sino también algunas otras propiedades tales como la calidad del servicio, aspectos concretos de seguridad adoptados por los dispositivos y las relaciones sociales en IoT.

Como trabajo futuro creemos interesante profundizar en nuestro trabajo sobre el sistema de ayuda a la toma de decisiones de seguridad en el cloud, llevando a cabo experimentos de monitorización exhaustivos en el Intercloud usando diferentes técnicas, sobre diferentes servicios en diferentes proveedores de cloud, generando evaluaciones de seguridad basadas en nuestra ontología SOFIC. También estamos planeando mejorar una implementación cloud existente, como OpenStack, con un mecanismo de reacción para proporcionar medidas de seguridad adecuadas, tales como la autoconfiguración de redes o migración dinámica de recursos y servicios, dando respuesta a las conclusiones inferidas por el sistema de ayuda a la decisión descrito en esta tesis.

Asimismo, sería interesante adaptar y ampliar nuestro sistema de control de acceso y la taxonomía de relaciones de confianza con el fin de abordar no sólo escenarios intra-cloud, sino también escenarios del Intercloud. También creemos que sería interesante abordar otros nichos de investigación relacionados con la seguridad en el Intercloud, ya que las posibilidades que abre este campo son enormes. En este sentido nos gustaría vincular nuestro sistema Trust-DSS con otras áreas de seguridad como la gestión de identidad. De esta forma los índices de confianza y las expectativas de seguridad deducidas por el sistema Trust-DSS podrían ser utilizadas por un sistema de gestión de identidad con capacidades de preservar la privacidad. Este sistema permitiría a los usuarios usar de forma dinámica sus diferentes identidades parciales digitales, y a su vez los atributos de identidad revelados en cada momento, teniendo en cuenta las deducciones del sistema Trust-DSS.

Abstract

I Motivation and Goals

IT systems are continuously evolving to cope with the incredible increase of society demands. This trend is leading the distributed systems to a new stage where infrastructures and flexible services need to scale up and down to deliver their services timely and on demand. The Cloud Computing [10] paradigm addresses these issues enabling an efficient provisioning of virtual IT architectures, where resources are dynamically created and dismantled according to customer needs. Cloud Computing is foremost characterized by its ubiquituous access, ondemand service provision, elasticity and resource pooling.

Cloud Computing, like any other kind of distributed system, has to face different challenges regarding security, such as authentication, authorization, privacy and trust management [113]. However, although there are some initial proposals and implementations to manage security aspects in Cloud Computing, there is a lack of advanced and high expressive authorization and trust models specially meant for this emerging parading, where the multi-tenancy characteristic [90] raises new security risks and authorization necessities. Current authorization and trust management solutions deployed in Cloud Computing have been directly taken from previous designs, and therefore, they are not yet totally adapted to cope with these new scenarios.

Security management in distributed systems like Cloud Computing, can be carried out by means of applying security policies and rules over system and security models enriched semantically. The Semantic Web [22] approach allows performing deductive reasoning and inference processes to come up with meaningful security conclusions which, in turn, can be used to make authorization and trust decisions and, ultimately, to react and adapt the system accordingly.

In this sense, the Semantic Web can be employed to drive the management of a high expressive authorization system, enabling advanced features required, and not yet fully addressed in Cloud Computing. A novel advanced access control model might take the advantage of the logic formalism provided by the Semantic Web technologies to describe the underlying infrastructure and authorization models, as well as the rules employed to protect the access to resources in the cloud.

The authorization system is of paramount importance to manage the access control of different cloud tenants to their associated resources. Nonetheless, in addition to the management of access control independently for each tenant, cloud tenants within the same cloud may need to collaborate to meet client demands, which requires new authorization and trust relationships models to manage such intra-cloud collaborations. For instance, let us assume that two or-

ganizations offering their services in the cloud reach a business agreement to offer a common new service that requires the usage of their current services. Both partners are different cloud tenants that use their corresponding cloud computational resources to run their part of the common service. In case one of them runs out of enough compute resources, it can use the other's computing resources to scale-up and continue providing the common service. This way, the organizations take advantage of this agreement to share cloud resources avoiding the need to rent more cloud resources from the CSP for the common service.

Nonetheless, these collaboration agreements are not supported in the current cloud and there is a lack of a proper trust model to restrict the information available across tenants which share the same underlying cloud infrastructure. This trust model should enable the establishment of alliances among them resulting in federation and coalition agreements. Thus, the cloud stack should be able to support this situation by enabling collaborative agreements between cloud customers. Nonetheless, these collaborations entail new security risks, since participating entities should trust each other to share their resources. The management of trust relationships in the cloud is gaining importance as a key element to establish a secure environment where entities are given full control in the definition of which particular services or resources are willing to share. Entities can cooperate at different levels of trust, according to their willingness of sharing information. In this regard, we think that these collaboration agreements have not yet addressed and studied enough in the state of the art, leading to different research opportunities.

On the other hand, vendor lock-in barrier makes it difficult for cloud customers to migrate data and applications across different clouds in a reliable and secure way. This is driving the need for flexible, dependable and secure Cloud Computing that operates beyond a single Cloud Service Provider (CSP) domain. This situation creates a need for new solutions that allow different CSPs to be interoperable with each other in a secure manner, coming up with federations of clouds, also known in the literature as Intercloud [23]. Such an interoperable environment enables both, customers and providers to interact with different clouds and compare cloud offerings such as pricing, quality of service and security capabilities to choose the most cost-effective one. At the same time, CSPs are starting to require the establishment of dynamic collaborations to deal with peaks of customers demands regarding computing, storage and networking. From the point of view of the CSP, the establishment of dynamic cloud federations can allow them to manage efficiently their cloud assets as well as offer economy of scale and enlargement of the provided capabilities.

However, the Intercloud environment is still in its earliest stages and therefore there exist plenty of areas of interest [44]. Namely, portability and migration, interoperability and APIs, support for building, modeling, testing and deploying applications, regulations and definition of Service Level Agreements (SLAs) as well as data protection, privacy and security. Although there exist some research works, initiatives and standards aimed to cope with different interoperability issues regarding the Intercloud, they are mainly focused on providing data models and interfaces for interoperability issues at Infrastructure as a Service (IaaS) layer of the stack, rather than providing the security models for the Intercloud. Therefore, there is a need for new approaches that allow different clouds to interoperate securely and in a reliable way with the aim of providing a trusted heterogeneous multidomain environment.

Among these security issues the analysis of the security and trust of a given CSP in order to establish reliable collaborations is an open research field that sparks a lot of interest. Despite there are others trust models to quantify the reliability and trustworthy of a given cloud entity or service, they do not actually define a broad set of security properties that should be considered by the trust model, and do not base their trust quantification on real security assessments about the CSP or Service. Rather, they base their quantification only on previous interactions and opinions gather from other sources.

The security assessed information could be exchanged afterwards in the Intercloud. In this sense, Semantic Web technologies could be employed as a way of exchange security information about a given CSP. The usage of ontologies, unlike others ways of expressing taxonomies and models, allows a high level of interoperability between different CSPs. In this sense, to the best of our knowledge, there is no any security ontology specially meant for the Intercloud.

Additionally, clients and CSPs could also take advantage of a trust and security decision support system for the Intercloud in order to make security decisions accordingly, such as dismiss or avoid interactions with certain CSPs or services based on these deductions. However, current cloud solutions for the Intercloud does not support this kind of security features. Moreover, such a trust and security decision support system could make use of the security ontology and the Semantic Web techniques to help on the security decision making process and determine whether a given CSP can be trusted in a a given context.

Cloud Computing is being applied in different scenarios in order to leverage their chances of success. Among the scenarios with highest possibilities we find all those related to the Internet of Things paradigm (IoT) [11]. Under the IoT vision, millions of interconnected devices, and their associated services, generate vast amount of data that are processed and analysed with different purposes, e.g. pattern recognition in such data. The success of the IoT services can be achieved as long as they are featured with ubiquitous accessibility, efficiency, reliability (handling the changes in context/policies and managing trust among entities and services), high performance, and scalability (since many resources and data may be involved in the service provision). The Cloud Computing characteristics mentioned at the beginning meet these IoT services requirements, and therefore, Cloud Computing is essential for today's IoT world.

In IoT heterogeneous devices are continuously exchanging information and being accessed ubiquitously through lossy networks. The IoT requires adapted trust quantification models in order to provide a reliable environment, thereby enabling unknown smart objects to interact each other in a trusted way. Besides, IoT has to deal with not only traditional access control mechanisms based on platform centric communications, but also in machine to machine (M2M) ones. Thus, access control models in IoT should be more lightweight to address the direct communication requirements of constrained devices, taking into account target devices' trust values prior any transaction. Likewise, trust quantification models should take into account different factors, beyond reputation, to work out trustworthiness. In this regard, in the current state of the art there is a lack of advanced trust models specially devised for the IoT, that can take into account, among other characteristics, a broader set of aspects and considerations to quantify trustworthiness of a given device.

Due to the challenges of trust management and authorization in distributed environments highlighted above, the general objectives of this PhD Thesis can be summarised in two. The main general aim is to make Cloud Computing more reliable by means of designing and implementing advanced authorization and trust models that rely on Semantic Web technologies. Likewise, the second goal is to provide a trust model targeting to more decentralized scenarios, like those derived from the Internet of Things, levering current IoT access control approaches in order to allow them to take into account the trust deductions.

In particular, the concrete goals pursued within this thesis, and derived from the two main objectives described above, are the following:

- Analyse and design a novel and high expressive authorization model specially meant for Cloud Computing relying on Semantic Web technologies.

- Analyse and design the trust relationships in Cloud Computing between cloud tenants in order to establish a reliable environment.

- Analyse the state of the art of security and trust in distributed systems, Cloud Computing and the Intercloud.

- Analyse the security requirements in Cloud Computing and define accordingly a full Intercloud security taxonomy and ontology.

- Design, implement and validate a trust and security decision support system, relying on Semantic Web techniques, in order to assist in the Intercloud security decision making process, quantify security expectations and trustworthiness about CSPs.

- Devise and implement an advanced trust model for Internet of Things to allow making authorization decisions based on this quantified trust values.

II Methodology

This PhD Thesis started by performing a survey of the current state of the art on security management in distributed systems. By then, we had already realized that a policy-based approach was a promising and emerging way to manage the security of complex IT systems. Under this administrative approach distributed systems can be managed efficiently while maintaining a proper order, security and consistency. At the same time, the Semantic Web paradigm had evolved enough to be used as a mechanism to enrich semantically the system models and the security polices, leveraging the management possibilities. Thus, we started to research about employing Semantic Web techniques to security management of distributed systems. It allowed us to start defining system and security models and performing reasoning over them using semantic policy rules, coming up with a powerful mechanism to manage the security of distributed systems.

Concretely, during the state of the art analysis we discovered that there was a lack of a high expressive authorization model based on the Semantic Web, that would be able to handle the complexity of distribute systems like Cloud Computing. Current authorization models for distributed systems are efficient, but at the same limited by their poor semantics, and therefore, by their limited authorization features. Thus, among the plethora of open research security topics in distributed systems, we started by focusing on the policy-based management of authorization in distributed systems, and following a Semantic Web approach.

Thus, after studying the applicability of Semantic Web techniques for authorization in Cloud Computing, we proposed an authorization model to address this challenge (Chapter 1). This authorization model, in contrast to traditional ones, is based on the Semantic Web, so that it enables performing inference reasoning to come up with meaningful security conclusions that can be used to make authorization decisions. Moreover, thanks to the usage of ontologies and semantic rules to model the authorization behavior, it allows providing advanced authorization features like hierarchical RBAC (hRBAC), conditional RBAC (cRBAC) and hierarchical objects (HO).

During the research carried out to devise the authorization model, we found that there was a lack of an study, and a formal model, to define the trust relationships established among tenants. Cloud tenants within the same cloud can collaborate each other to establish alliances and set up coalition agreements. Nonetheless, these agreements raise new security challenges, such as intra-cloud access control management. Customers should have means to establish coalition agreements while restricting the information available among other cloud tenants sharing the same underlying infrastructure. The problem of sharing the same infrastructure among different tenants is derived by the multi-tenancy nature of Cloud Computing. However, current cloud solutions do not allow managing these kind of collaborations and there exist a lack of a formal study regarding the kinds of trust relationships and their implications.

To bridge this gap, we performed an analysis and study of the different kind of collaborations that may occur among cloud tenants, coming up with a taxonomy defining different levels of trust relationships among customers of the cloud (Chapter 2). The taxonomy of trust relationships takes into account privacy concerns, assumed risk, as well as easiness in the definition of the agreements. The trust relationships can be, in the end, enforced by applying a proper authorization model that take into account these kind of agreements.

Furthermore, in addition to intra-cloud relationships among tenants, customers and CSPs are starting to require Intercloud scenarios where different clouds have to interact each other beyond one single cloud domain. Although there are some proposals to manage the Intercloud, there are still few approaches dealing with the associated new security and trust challenges in such a federated environment. In order to address this problem, we made a deep analysis of the state of the art in the Intercloud, analyzing the security and trust in this distributed environment. As a result we came up with an ontology aimed to formally describe the security aspects that are subject to be modelled in an Intercloud security assessment (Chapter 3). The ontology is based on security standards and it has been tailored extensible to cope with the security requirements of different Intercloud scenarios.

Besides, the ontology is used as input for a novel Trust and Security Decision Support System (Trust-DSS), in order to assist in the Intercloud security decision making process, quantifying security expectations and trustworthiness about Cloud Service Providers. Since the Trust-DSS is based on the Semantic Web it is able to perform inference over the security ontology and semantic rules in order to detect anomalous security situations and conflicts present in the assessments. As a result, it allows helping in decisions such as dismissing or avoiding interactions with certain CSPs or cloud services relying on these deductions.

Finally, we wanted to address the access control and trust management challenge not only in enterprise-centric distributed systems like Cloud Computing, but also in more decentralized ones. In this sense, the emerging Internet of Things paradigm is characterized by their lossy networks and machine to machine (M2M) communications that require the adaptation of current trust and authorization models. The traditional enterprise-centric approach requires a continuous intervention of an online Policy Decision Point (PDP) entity in charge of making authorization decisions, which is a drawback for IoT scenarios. Thereby, we made an analysis of the state of the art of trust models for IoT as well as authorization models that could take into account trust scores in M2M scenarios. The goal was to improve the reliability in IoT scenarios, where initially unknown devices are prone to interact with each other. As a result of this analysis, we realized that there were not any trust model specially devised for the IoT scenarios that could be enforced along with an authorization model also designed for IoT. Hence, we designed a security mechanism to leverage an already existing IoT authorization system called DCapBAC [60], with our novel trust model that takes into account not only reputation, as it is commonly employed in traditional peer to peer (P2P) scenarios, but also some other advanced aspects to quantify trust (Chapter 4).

III Results

This PhD Thesis was conceived from the beginning as a compilation of a set of publications, so that the results are essentially exposed in the articles that compose it. The first results derived from the analysis and design of a semantic-aware access control system for Cloud Computing was presented in the International Conference on Security and Cryptography (SECRYPT), in a paper entitled “Towards an Authorization System for Cloud Infrastructure Providers” [19].

In such a paper we presented the authorization system for Cloud Computing that addresses the multi-tenancy characteristic of Cloud Computing. The proposal is based on Semantic Web technologies, with SWRL[61] rules and a system model definition that is represented as an OWL[54] ontology derived from the Common Information Model (CIM) [28] standard. We demonstrated that Semantic Web technologies are useful for describing authorization models for distributed systems. In the end it allows inferring new knowledge and supporting different authorization features overcoming certain lacks of expressiveness of its predecessors, such as role based access control (RBAC), hierarchical RBAC (hRBAC), conditional RBAC (cRBAC) and hierarchical objects (HO).

Next, we investigated further into the different kinds of trust relationships that can occur in Cloud Computing, and the outcome was reflected in the article entitled "Taxonomy of trust relationships in authorization domains for Cloud Computing" [85], which was published in The Journal of Supercomputing. The accomplished analysis ended up with a formal description of the different trust relationships in Cloud Computing, enabling the definition of different collaboration agreements in different scenarios. Additionally, this work presents a comparison of all these trust relationships, analyzing aspects such as privacy control, risk assumed, trust level and easiness of management. A trust management architecture has been also devised allowing tenants to make use of the trust relationship definitions in order to manage and control the collaboration agreements between them. The architecture has been validated by means of a prototype implemented using Semantic Web technologies. The paper also presented a diverse set of common scenarios in Cloud Computing, proposing the most convenient trust relationships for each case.

The research carried out regarding trust and security in the Intercloud is shown in the paper "Intercloud Trust and Security Decision Support System: an Ontology-based approach" [68], which is currently in press in the Journal of Grid Computing. In this work we have analyzed and identified the security areas, properties and metrics required when assessing the security of a CSP. These concepts have been modeled in the SOFIC ontology [121] to support a high degree of interoperability in the Intercloud. Besides, the ontology can be taken as a starting point to quantify expectations and trust values of cloud services as well as supporting CSPs and tenants in the Intercloud security decision making process. The SOFIC ontology has been released making it open and public, it is based on standards and has been devised extensible and adaptable in order to deal with the security requirements of different Intercloud scenarios.

The research regarding the Intercloud have shown the advantages of having an OWL ontology to model security aspects of Cloud Computing. A set of experiments have been conducted in order to validate the performance and feasibility the Trust and Security Decision Support System (Trust-DSS) implementation. In this sense it is able to handle properly more than an enough amount of historical assessments about CSPs. Besides, it shows how can it be performed efficiently a Semantic Web based trust and security decision making process, based on SWRL rules, in order to check security constraints and conflicts, thereby allowing to dismiss or avoid interactions with certain CSPs or cloud services that may be unreliable. The paper evidences the ability of the proposal to deduce security expectations values about different security aspects. Moreover, the Trust-DSS also provides a trust model to quantify efficiently trust indexes about cloud services relying on an arithmetic and fuzzy approach, which takes into account historical assessments and certainty.

Finally, regarding the trust model for the Internet of Things, our research results were published in the Soft Computing journal, in a paper entitled "TACIoT: multidimensional trust-aware access control system for the Internet of Things" [21]. The paper provides a trust model leveraging the DCapBAC[60] access control system to take into account devices' trust values to make authorization decisions accordingly. The trust model is especially designed for IoT, taking into account, four dimensions, i.e., quality of service, reputation, security aspects and social relationships, to compute trust values about IoT devices. TACIoT was implemented making use of a fuzzy control system, which relies on the four trust dimensions, which in turn, are quantified from historical trust properties evidences. The experiments conducted show the feasibility of the research when testing the implementation on real IoT scenarios for constrained and non-constrained devices. The achieved results show reasonable times when performing the trust-aware access control process for both kinds of devices.

IV Conclusions and Future Work

Cloud Computing is rapidly evolving to meet new client demands. Nonetheless, besides the wide range of opportunities provided by this new paradigm, there exist, unfortunately, several risks associated to its incredible development. Although traditional security solutions regarding authorization and trust management have been proven to be fairly effective in previous scenarios, the impressive expansion of the cloud along with their new security necessities make them not totally suitable for Cloud Computing and Intercloud scenarios.

Establishing a reliable and trusted cloud environment is an open issue that still requires a collaborative effort to succeed. The multi-tenancy and virtualization nature of Cloud Computing raises new security concerns, and customers require new updated mechanisms to increase the reliability, security and confidence in this distributed environment. In this sense, Cloud Computing requires more high expressive authorization models in order to overcome certain lacks of its predecessors. Endowing Cloud Computing with federation capabilities to support trust relationships among customers is an open research topic not addressed yet in the current state of the art. Additionally, current trust models for the Intercloud are not based on real security assessments performed over the Cloud Service Providers, which allow coming up with a powerful way to evaluate CSPs and make security decisions accordingly.

In this PhD thesis, a set of solutions has been proposed, analyzed and implemented in order to enhance the digital trust in Cloud Computing and overcome the aforementioned open issues. Firstly, we have proposed a high expressive semantic-aware access control system which enables advanced authorization features.

To deal with collaboration agreements established in Cloud Computing we have proposed a formal description of the different kind of trust relationships that can occur in different scenarios. We have made an interesting analysis and comparison of the different kind of trust relationships and their suitability to common scenarios in Cloud Computing, taking into account different key aspects such as privacy control, risk assumed, trust level and easiness of management.

Additionally, we have proposed a trust and decision support system (Trust-DSS) for the Intercloud together with the SOFIC security ontology. It is an interesting result for any cloud customer since it endows them with mechanisms to work out dynamically security expectations and trustworthiness of a given CSP. In the end, it allows them to drive their behavior according to the Trust-DSS conclusions and increase their security and trust in Cloud Computing.

Furthermore, a trust model for the Internet of Things can quantify trust scores by gathering different kind of information from different sources. It can allow devices generating its own opinion about how trustworthy another "thing" is, when performing a specific action in a given context. The trust values can be taken into account in the moment of making authorization decision, reducing possible harmful attacks. In this regard, this thesis has also provided and evaluated an advanced trust model specially tailored for IoT that follows a multidimensional approach to compute trust values about IoT devices. It takes into account not only reputation gathered from third entities, but also some other properties such as quality of service, actual security aspects and social relationships.

As future work, we envisage to deep into our research regarding the Trust-DSS, carrying out exhaustive monitoring experiments in the Intercloud over different services at different CSPs to generate security assessments following the our SOFIC ontology. We are also planning to improve a cloud stack implementation, like OpenStack, with a reaction mechanism to provide security countermeasures, such as dynamic firewall configuration or services migration to other clouds, based on the conclusions inferred by the Trust and Security Decision Support System described in this thesis.

We are also planning to address some other open research issues in the Intercloud. In this sense, we expect to adapt and extend our semantic-aware access control system and the trust relationships taxonomy in order to cope with not only intra-cloud scenarios, but also Intercloud ones. Additionally, we envisage to link our Trust-DSS with some other Intercloud security areas such as Identity Management (IdM). In this regard, the trust scores and security expectations deduced by the Trust-DSS can be used by a privacy-by-design and user-centric IdM that would allow users to enforce dynamically their different digital faces, and in turn their disclosed identity attributes, according to the target cloud service, the context and the Trust-DSS deductions. Finalmente, nos gustaría abordar la gestión de la seguridad (control de acceso, confidencialidad..), privacidad y la confianza en burbujas de smart objects, las cuales pueden formarse oportunísticamente en base a diferentes tipos de relaciones, tal y como demandan algunos escenarios IoT.

Publications composing the PhD Thesis

1

Towards an Authorization System for Cloud Infrastructure Providers

Title:	Towards an Authorization System for Cloud Infrastructure Providers
Authors:	Jorge Bernal Bernabé, Juan Manuel Marín Pérez, Jose M. Alcaraz Calero, Félix J. García Clemente, Gregorio Martínez Pérez and Antonio F. Gómez Skarmeta.
Type:	Conference
Conference:	SECRYPT 2011 - Proceedings of the International Conference on Security and Cryptography
Publisher:	IEEE
ISBN:	978-989-8425-71-3
Pages:	333 - 338
Year:	2011
Month:	July
State:	Published
DOI:	http://dx.doi.org/10.5220/0003525703330338

Table 1: Towards an Authorization System for Cloud Infrastructure Providers

Abstract

The provision of security services is a key enabler in cloud computing architectures. Focusing on multitenancy authorization systems, the provision of different models including role based access control (RBAC), hierarchical RBAC (hRBAC), conditional RBAC (cRBAC) and hierarchical objects (HO) is the main objective of this paper. Our proposal is based on the Common Information Model (CIM) and Semantic Web technologies, which have been demonstrated as valid tools for describing authorization models. As the same language is being used for the information and the authorization models they are both well aligned and thus reducing the potential mismatch that may appear between the semantics of both models. A trust model enabling the establishment of coalitions and federations across tenants is also an objective being covered as part of the research being presented in this paper

2

Taxonomy of trust relationships in authorization domains for cloud computing

Title:	Taxonomy of trust relationships in authorization domains for cloud computing
Authors:	Juan Manuel Marín Pérez, Jorge Bernal Bernabé, Jose M. Alcaraz Calero, Félix J. García Clemente, Gregorio Martínez Pérez and Antonio F. Gómez Skarmeta.
Type:	Journal
Journal:	The Journal of Supercomputing
Impact factor (2014):	0.858 Q3
Publisher:	Springer
Volume:	70
Number:	3
Pages:	1075-1099
Year:	2014
Month:	December
DOI:	http://dx.doi.org/10.1007/s11227-014-1117-x
State:	Published

Table 2: Taxonomy of trust relationships in authorization domains for cloud computing

Abstract

Cloud computing is revealing a new scenario where different cloud customers need to collaborate to meet client demands. The cloud stack must be able to support this situation by enabling collaborative agreements between cloud customers. However, these collaborations entail new security risks since participating entities should trust each other to share a set of resources. The management of trust relationships in the cloud is gaining importance as a key element to establish a secure environment where entities are given full control in the definition of which particular services or resources they are willing to share. Entities can cooperate at different levels of trust, according to their willingness of sharing information. This paper analyses these collaboration agreements defining a taxonomy of different levels of trust relationships among customers for the cloud. Privacy concerns, assumed risk, as well as easiness in the definition of the trust relationships have been taken into account. A set of different trust relationships have been identified and modeled, enabling entities to control the information they share with others in the cloud. The proposed model has been validated with a prototypical implementation. Likewise, some examples to illustrate the application of these trust models to common cloud collaboration scenarios are provided.

3

Intercloud Trust and Security Decision Support System: an Ontology-based approach

Title:	Intercloud Trust and Security Decision Support System: an Ontology-based approach
Authors:	Jorge Bernal Bernabé, Gregorio Martínez Pérez, Antonio F. Gómez Skarmeta
Type:	Journal
Journal:	Journal of Grid Computing
Impact factor (2015):	1.5 Q1
Publisher:	Springer
Volume:	
Number:	
Pages:	
Year:	2015
Month:	
DOI:	http://dx.doi.org/10.1007/s10723-015-9346-7
State:	In press, Published Online

Table 3: Intercloud Trust and Security Decision Support System: an Ontology-based approach

Abstract

As Cloud Computing evolves, both customers and Cloud Service Providers are starting to require Intercloud scenarios where different clouds have to interact each other. Although there are some initial proposals to manage the Intercloud, there are still few approaches dealing with the associated new security and trust challenges in such a federated environment. To fill this gap, this paper presents SOFIC (Security Ontology For the InterCloud) aimed to formally describe the security aspects that are subject to be modeled in an Intercloud security assessment. SOFIC is based on standards and has been tailored extensible to cope with the security requirements of different Intercloud scenarios. Thepaper also shows in which way the ontology is used as input for a Trust and Security Decision Support System, in order to assist in the Intercloud security decision making process, quantifying security expectations and trustworthiness about Cloud Service Providers. The implementation, experiments and performance evaluation show the feasibility of the proposed ontology and system.

4

TACIoT: multidimensional trust-aware access control system for the Internet of Things

Title:	TACIoT: multidimensional trust-aware access control system for the Internet of Things
Authors:	Jorge Bernal Bernabé, Jose Luis Hernández Ramos and Antonio F. Skarmeta Gómez .
Type:	Journal
Journal:	Soft Computing
Impact factor (2014):	1.27 Q3
Publisher:	Springer
Volume:	
Number:	
Pages:	
Year:	2015
Month:	May
DOI:	http://dx.doi.org/10.1007/s00500-015-1705-6
State:	In Press, Published Online

Table 4: TACIoT: multidimensional trust-aware access control system for the Internet of Things

Abstract

Internet of Things environments are comprised of heterogeneous devices that are continuously exchanging information and being accessed ubiquitously through lossy networks. This drives the need of a flexible, lightweight and adaptive access control mechanism to cope with the pervasive nature of such global ecosystem, ensuring, at the same time, reliable communications between trusted devices. To fill this gap, this paper proposes a flexible trust-aware access control system for IoT (TACIoT), which provides an endto- end and reliable security mechanism for IoT devices, based on a lightweight authorization mechanism and a novel trust modelthat has been specially devised for IoT environments. TACIoT extends traditional access control systems by taking into account trust values which are based on reputation, quality of service, security considerations and devices' social relationships. TACIoT has been implemented and evaluated successfully in a real testbed for constrained and non-constrained IoT devices.

Bibliography

[1] Creating a socially aware citizen-centric Internet of Things. Eu fp7 sociotal project, 2013.

[2] Jemal Abawajy. Determining service trustworthiness in inter loud computing environments. In *ISPAN 2009 : Proceedings of the 2009 10th International Symposium on the Pervasive Systems, Algorithms and Networks*, pages 784–788, 2009.

[3] Imad M. Abbadi and Andrew Martin. Trust in the cloud. *Information Security Technical Report*, 16(3):108–114, 2011.

[4] ImadM. Abbadi. A framework for establishing trust in cloud provenance. *International Journal of Information Security*, 12(2):111–128, 2013.

[5] Giuseppe Aceto, Alessio Botta, Walter De Donato, and Antonio Pescapè. Survey cloud monitoring: A survey. *Comput. Netw.*, 57(9):2093–2115, June 2013.

[6] Jose M. Alcaraz-Calero, Nigel Edwards, Johannes Kirschnick, Lawrence Wilcock, and Mike Wray. Towards a multi-tenancy authorization system for cloud services. *IEEE Security and Privacy*, 8(6):48–55, Nov 2010.

[7] Jose M. Alcaraz-Calero, Gregorio Martinez Perez, and Antonio F. Gomez Skarmeta. Towards an authorization model for distributed systems based on the semantic web. *IET Information Security*, 4(4):411–421, Dec 2010.

[8] D. Androcec, N. Vrcek, and J. Seva. Cloud computing ontologies: A systematic review. In *MOPAS 2012, The Third International Conference on Models and Ontology-based Design of Protocols, Architectures and Services*, 2012.

[9] Deliverable 3. Integrated System Architecture and Initial Pervasive BUTLER proof of concept. Eu fp7 butler project, 2013.

[10] Michael Armbrust, Armando Fox, Rean Griffith, Anthony D Joseph, Randy Katz, Andy Konwinski, Gunho Lee, David Patterson, Ariel Rabkin, Ion Stoica, et al. A view of cloud computing. *Communications of the ACM*, 53(4):50–58, 2010.

[11] L. Atzori, A. Iera, and G. Morabito. The internet of things: A survey. *Elsevier Computer Networks*, 54(15):2787–2805, 2010.

[12] Luigi Atzori, Antonio Iera, Giacomo Morabito, and Michele Nitti. The social internet of things (siot)–when social networks meet the internet of things: Concept, architecture and network characterization. *Computer Networks*, 56(16):3594–3608, 2012.

[13] Paolo Balboni and et al. Procure secure, a guide to monitoring of security service levels in cloud contracts. Document, European Network and Information Security Agency, 2012.

[14] Fenye Bao and Ing-Ray Chen. Dynamic trust management for internet of things applications. In *Proceedings of the 2012 international workshop on Self-aware internet of things*, pages 1–6. ACM, 2012.

[15] Fenye Bao, Ing-Ray Chen, and Jia Guo. Scalable, adaptive and survivable trust management for community of interest based internet of things systems. In *Autonomous Decentralized Systems (ISADS), 2013 IEEE Eleventh International Symposium on*, pages 1–7. IEEE, 2013.

[16] Alessandro Bassi, Martin Bauer, Martin Fiedler, Thorsten Kramp, Rob van Kranenburg, Sebastian Lange, and Stefan Meissner. *Enabling Things to Talk*. Springer, 2013.

[17] Dave Beckett. Rdf/xml syntax specification. Technical report, W3C, 2004.

[18] Yosra Ben Saied, Alexis Olivereau, Djamal Zeghlache, and Maryline Laurent. Trust management system design for the internet of things: A context-aware and multi-service approach. *Computers & Security*, 39:351–365, 2013.

[19] Jorge Bernal Bernabe, Juan M. Marin Perez, Jose M. Alcaraz Calero, Felix J. Garcia Clemente, Gregorio Martinez Perez, and Antonio F. Gomez Skarmeta. Towards an authorization system for cloud infrastructure providers. In *Internacional Conference on Security and Cryptography*, pages 333–338, 2006.

[20] Jorge Bernal Bernabe, Juan M. Marin Perez, Jose M. Alcaraz Calero, and Antonio F. Gomez Skarmeta Felix J. Garcia Clemente, Gregorio Martinez Perez. Semantic-aware multi-tenancy authorization system for cloud architectures. *Future Generation Computer Systems*, 32:154–167, 2014.

[21] Jorge Bernal Bernabe, JoseLuis Hernandez Ramos, and AntonioF. Skarmeta Gomez. TACIoT: multidimensional trust-aware access control system for the Internet of Things. *Soft Computing*, pages 1–17, 2015.

[22] Tim Berners-Lee, James Hendler, Ora Lassila, et al. The semantic web. *Scientific american*, 284(5):28–37, 2001.

[23] D. Bernstein, E. Ludvigson, K. Sankar, S. Diamond, and M. Morrow. Blueprint for the intercloud - protocols and formats for cloud computing interoperability. In *Fourth International Conference on Internet and Web Applications and Services*, pages 328–336, 2009.

[24] David Bernstein and Vij Deepak. Intercloud security considerations. In *2nd IEEE International Conference on Cloud Computing Technology and Science*, pages 537–544, 2010.

[25] David Bernstein and Tony Li. P2302 Standard for Intercloud Interoperability and Federation. Technical report, IEEE, 2012.

[26] Carlos Blanco, Joaquin Lasheras, Rafael Valencia-García, Eduardo Fernández-Medina, Ambrosio Toval, and Mario Piattini. A systematic review and comparison of security ontologies. In *Proceedings of the 2008 Third International Conference on Availability, Reliability and Security*, ARES '08, pages 813–820, Washington, DC, USA, 2008. IEEE Computer Society.

[27] Latifa Boursas and Wolfgang Hommel. Multidimensional dynamic trust management for federated services. *Computational Science and Engineering, IEEE International Conference on*, 2:684–689, 2009.

[28] Winston Bumpus, John W. Sweitzer, Patrick Thompson, AndreaR. Westerinen, and Raymond C. Williams. *Common information model: implementing the object model for enterprisemanagement*. John Wiley & Sons, Inc, 2000.

[29] Jose M. Alcaraz Calero, Juan M. Marin Perez, Jorge Bernal Bernabe, Felix J. Garcia Clemente, Gregorio Martinez Perez, and Antonio F. Gomez Skarmeta. Detection of semantic conflicts in ontology and rule-based information systems". *Data & Knowledge Engineering*, 69(11):1117 – 1137, 2010. Special issue on contribution of ontologies in designing advanced information systems.

[30] Jeremy J. Carroll, Ian Dickinson, Chris Dollin, Dave Reynolds, Andy Seaborne, and Kevin Wilkinson. Jena: Implementing the semantic web recommendations. In *Proceedings of the 13th international World Wide Web conference*, pages 74–83. ACM Press, 2004.

[31] A. Celesti, F. Tusa, M. Villari, and A. Puliafito. How to enhance cloud architectures to enable cross-federation. In *Cloud Computing (CLOUD), 2010 IEEE 3rd International Conference on*, pages 337–345, 2010.

[32] DavidW. Chadwick, Kristy Siu, Craig Lee, Yann Fouillat, and Damien Germonville. Adding federated identity management to openstack. *Journal of Grid Computing*, 12(1):3–27, 2014.

[33] Dong Chen, Guiran Chang, Dawei Sun, Jie Jia, and Xingwei Wang. Modeling access control for cyber-physical systems using reputation. *Computers & Electrical Engineering*, 38(5):1088–1101, 2012.

[34] Dong Chen, Guiran Chang, Dawei Sun, Jiajia Li, Jie Jia, and Xingwei Wang. Trm-iot: A trust management model based on fuzzy reputation for internet of things. *Computer Science and Information Systems*, 8(4):1207–1228, 2011.

[35] D. Crockford. RFC 4627: The application/json Media Type for Javascript Object Notation (JSON). IETF RFC 4627, July 2006. http://www.ietf.org/rfc/rfc4627.txt.

[36] CSA. Security guidance for critical areas of focus in cloud computing. Technical report, Cloud Security Alliance (CSA), 2012.

[37] CSA. Cloud controls matrix. Document, Cloud Security Alliance, 2013.

[38] Chen Danwei, Huang Xiuli, and Ren Xunyi. Access control of cloud service based on ucon. *LNCS Cloud Computing*, 5931:559–564, 2009.

[39] Markus Debusmann and Alexander Keller. SLA-driven management of distributed systems using the common information model. In *Proceeding of the 8th IFIP/IEEE International Symposium on Integrated Network Management*, 2003.

[40] DMTF. Cloud Infrastructure Management Interface (CIMI) Model and RESTful HTTP-based Protocol. An Interface for Managing Cloud Infrastructure. Specification DSP0263, Distributed Management Task Force, 2012.

[41] Jiaqing Du, Nipun Sehrawat, and Willy Zwaenepoel. Performance profiling of virtual machines. *SIGPLAN Not.*, 46(7):3–14, March 2011.

[42] Robert Dukaric and Matjaz B. Juric. Towards a unified taxonomy and architecture of cloud frameworks. *Future Generation Computer Systems*, 29(5):1196 – 1210, 2013.

[43] Paolo Balboni et al. Security and privacy controls for federal information systems and organizations. Special publication SP 800-53 rev4, National Institute of Standards and Technology, 2012.

[44] ETSI. Initial analysis of standardization requirements for cloud services. Technical Report ETSI TR 102 997, European Telecommunications Standards Institute, 2010.

[45] Faiza Fakhar and Muhammad Awais Shibli. Comparative analysis on security mechanisms in cloud. In *2013 15th International Conference on Advanced Communication Technology (ICACT)*, pages 145–50, 2013.

[46] Doudou Fall, Gregory Blanc, Takeshi Okuda, Youki Kadobayashi, and Suguru Yamaguchi. Toward quantified risk-adaptive access control for multi-tenant cloud computing. In *The 6th Joint Workshop on Information Security*, pages 1–14, 2011.

[47] D. Ferraiolo, J. Cugini, and R. Kuhn. Role-based access control (RBAC): Features and motivations. In *Proc. of 11th Annual Computer Security Application Conference*, pages 241–48, 1995.

[48] Laurence Field, Shiraz Memon, Iván Márton, and Gábor Szigeti. The emi registry: Discovering services in a federated world. *Journal of Grid Computing*, 12(1):29–40, 2014.

[49] Mohamed Firdhous, Osman Ghazali, and Suhaidi Hassan. Trust management in cloud computing: A critical review. *International Journal on Advances in ICT for Emerging Regions (ICTer)*, 4(2):24–36, 2012.

[50] T.-F. Fortis, V.I. Munteanu, and V. Negru. Towards an ontology for cloud services. In *Complex, Intelligent and Software Intensive Systems (CISIS), 2012 Sixth International Conference on*, pages 787–792, 2012.

[51] Ian Foster, Yong Zhao, Ioan Raicu, and Shiyong Lu. Cloud computing and grid computing 360-degree compared. In *Grid Computing Environments Workshop*, pages 1–10. IEEE, IEEE, Nov 2008.

[52] Feng Fujun and Li Junshan. Trust based authorization and access control. In IEEE, editor, *2009 International Forum on Information Technology and Applications*, pages 162–165, 2009.

[53] S. Gerdes. Actors in the ace architecture. *IETF Internet Draft, draft-gerdes-ace-actors-01*, 2014.

[54] W3C OWL Working Group. OWL 2 Web Ontology Language: Document overview (second edition). W3C recommendation, W3C, December 2012.

[55] S. Gusmeroli, S. Piccione, and D. Rotondi. A capability-based security approach to manage access control in the internet of things. *Mathematical and Computer Modelling*, 58(5-6):1189–1205, September 2013.

[56] Keiko Hashizume, DavidG Rosado, Eduardo Fernández-Medina, and EduardoB Fernandez. An analysis of security issues for cloud computing. *Journal of Internet Services and Applications*, 4(1):1–13, 2013.

[57] Brian Hayes. Cloud computing. *Communications of the ACM*, 51(7):9–11, 2008.

[58] Tobias Heer, Oscar Garcia-Morchon, René Hummen, Sye Loong Keoh, Sandeep S Kumar, and Klaus Wehrle. Security challenges in the ip-based internet of things. *Wireless Personal Communications*, 61(3):527–542, 2011.

[59] D. Heimbigner. DMTF - CIM to OWL: A Case Study in Ontology Conversion. In *Conference on Software Engineering and Knowledge Engineering*, 2004.

[60] José L Hernández-Ramos, Antonio J Jara, Leandro Marín, and Antonio F Skarmeta. Dcapbac: Embedding authorization logic into smart things through ecc optimizations. *International Journal of Computer Mathematics*, (just-accepted):1–22, 2014.

[61] I. Horrocks, P. F. Patel-Schneider, H. Boley, S. Tabet andB. Grosof, and M. Dean. SWRL: A Semantic Web Rule Language combining OWL and RuleML. Technical report, W3C, 2004.

[62] Donghui Hu, Lina Wang, Yu Zhou, Yang Zhou, Xiaqiu Jiang, and Longfei Ma. D-s evidence theory based digital image trustworthiness evaluation model. In *Proceedings of the 2009 International Conference on Multimedia Information Networking and Security - Volume 01*, MINES '09, pages 85–89, Washington, DC, USA, 2009. IEEE Computer Society.

[63] Luokai Hu, Shi Ying, Xiangyang Jia, and Kai Zhao. Towards an approach of semantic access control for cloud computing. *LNCS Cloud Computing*, 5931:145–156, 2009.

[64] Rong Hu, Jianxun Liu, and Xiaoqing Frank Liu. A trustworthiness fusion model for service cloud platform based on d-s evidence theory. *Cluster Computing and the Grid, IEEE International Symposium on*, 0:566–571, 2011.

[65] M. Victoria Moreno J. Bernal Bernabé, J. Luis Hernández and A. Skarmeta. Privacy-preserving security framework for a social-aware internet of things. In *UCAmI 2014*, pages 408–415. 2014.

[66] Wayne Jansen and Timothy Grance. Guidelines on security and privacy in cloud computing. Technical Report SP-800-14, National Institute of Standards and Technology, 2011.

[67] Antonio J Jara, Pablo Lopez, David Fernandez, Jose F Castillo, Miguel A Zamora, and Antonio F Skarmeta. Mobile digcovery: discovering and interacting with the world through the internet of things. *Personal and ubiquitous computing*, 18(2):323–338, 2014.

[68] Antonio F. Skarmeta Gómez. Jorge Bernal Bernabé, Gregorio Martínez Pérez. Intercloud Trust and Security Decision Support System: an Ontology-based Approach. *Journal of Grid Computing*, pages 1–32, 2015.

[69] et al Khasnabish. Cloud Reference Framework. Technical report, Internet Engineering Task Force.

[70] Anya Kim, Jim Luo, and Myong Kang. Security ontology to facilitate web service description and discovery. In Stefano Spaccapietra, Paolo Atzeni, François Fages, Mohand-Saïd Hacid, Michael Kifer, John Mylopoulos, Barbara Pernici, Pavel Shvaiko, Juan Trujillo, and Ilya Zaihrayeu, editors, *Journal on Data Semantics IX*, volume 4601 of *Lecture Notes in Computer Science*, pages 167–195. Springer Berlin Heidelberg, 2007.

[71] Ron Knode and Doug Egan. Into the cloud with ctp: A precis for the cloudtrust protocol. Technical report, Computer Sciences Corporation, 2010.

[72] Bo Lang, Zhibin Wang, and Qingwen Wang. Trust representation and reasoning for access control in large scale distributed systems. In IEEE, editor, *2nd International Conference on Pervasive Computing and Applications*, pages 436–441. IEEE, July 2007.

[73] Marc Langheinrich. Privacy by design principles of privacy aware ubiquitous systems. In *Ubicomp 2001: Ubiquitous Computing*, pages 273–291. Springer, 2001.

[74] Alexander Lenk, Markus Klems, Jens Nimis, Stefan Tai, and Thomas Sandholm. Whats inside the cloud? an architectural map of the cloud landscape. In *Proceeding at ICSE Workshop on Software Engineering Challenges of Cloud Computing*, pages 1–6, 2009.

[75] Ang Li, Xiaowei Yang, Srikanth Kandula, and Ming Zhang. Cloudcmp: Comparing public cloud providers. In *Proceedings of the 10th ACM SIGCOMM Conference on Internet Measurement*, IMC '10, pages 1–14, New York, NY, USA, 2010. ACM.

[76] Dancheng Li, Cheng Liu, Qiang Wei, Zhiliang Liu, and Binsheng Liu. Rbac-based access control for saas systems. In IEEE, editor, *2010 2nd International Conference on Information Engineering and Computer Science*, pages 1–4. IEEE, Dec 2010.

[77] XIAO-YONG LI, YONG SHI, and WEI MA YU-GUO. Multi-tenancy based access control in cloud. In IEEE, editor, *2010 International Conference on Computational Intelligence and Software Engineering*, volume 1, pages 1–4. IEEE, Dec 2010.

[78] Xiaoyong Li and Junping Du. Adaptive and attribute-based trust model for service level agreement guarantee in cloud computing. *Information Security, IET*, 7(1):39–50, 2013.

[79] P. N. Mahalle, B. Anggorojati, N. R. Prasad, and R. Prasad. Identity driven Capability based Access Control (ICAC) for the Internet of Things. In *Proc. of the 6th IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), Bangalore, India*, pages 49–54. IEEE, December 2012.

[80] Parikshit N Mahalle, Pravin A Thakre, Neeli Rashmi Prasad, and Ramjee Prasad. A fuzzy approach to trust based access control in internet of things. In *Wireless Communications, Vehicular Technology, Information Theory and Aerospace & Electronic Systems (VITAE), 2013 3rd International Conference on*, pages 1–5. IEEE, 2013.

[81] Marta Majewska, Bartosz Kryza, and Jacek Kitowski. Translation of Common Information Model to Web Ontology Language. *LNCS Computational Science - ICCS 2007*, 4487:414–417, 2007.

[82] P.D. Manuel, S. Thamarai Selvi, and M.I.A.-E. Barr. Trust management system for grid and cloud resources. In *Advanced Computing, 2009. ICAC 2009. First International Conference on*, pages 176–181, 2009.

[83] Hongyan Mao, Linpeng Huang, and Minglu Li. Web resource monitoring based on common information model. In *IEEE Asia-Pacific Conference on Services Computing*, 2006.

[84] L. Marin, A. Jara, and A. Skarmeta. Shifting primes on openrisc processors with hardware multiplier. In *Information and Communicatiaon Technology*, pages 540–549. Springer, 2013.

[85] JuanM. Marin Perez, Jorge Bernal Bernabe, JoseM. Alcaraz Calero, FelixJ. Garcia Clemente, Gregorio Martinez Perez, and AntonioF. Gomez Skarmeta. Taxonomy of trust relationships in authorization domains for cloud computing. *The Journal of Supercomputing*, 70(3):1075–1099, 2014.

[86] Felix Gomez Marmol and Gregorio Martinez Perez. Towards pre-standardization of trust and reputation models for distributed and heterogeneous systems. *Computer Standards and Interfaces*, 32(4):185 – 196, 2010.

[87] Sergio Marti and Hector Garcia-Molina. Taxonomy of trust: Categorizing p2p reputation systems. *Computer Networks*, 50(4):472–484, 2006.

[88] Tim Mather, Subra Kumaraswamy, and Shahed Latif. *Cloud security and privacy: an enterprise perspective on risks and compliance.* O'Reilly Media, 2009.

[89] Carlo Maria Medaglia and Alexandru Serbanati. An overview of privacy and security issues in the internet of things. In *The Internet of Things*, pages 389–395. Springer, 2010.

[90] Peter Mell and Tim Grance. The NIST definition of cloud computing. *Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology Gaithersburg*, 2011.

[91] F. Moscato, R. Aversa, B. Di Martino, T. Fortis, and V. Munteanu. An analysis of mosaic ontology for cloud resources annotation. In *Computer Science and Information Systems (FedCSIS), 2011 Federated Conference on*, pages 973–980, 2011.

[92] Monoj Kumar Muchahari and Smriti Kumar Sinha. A new trust management architecture for cloud computing environment. In *2012 International Symposium on Cloud and Services Computing*, pages 136–140, 2012.

[93] Kawser Wazed Nafi, Tonny Shekha Kar, Md. Amjad Hossain, and M. M. A. Hashem. An advanced certain trust model using fuzzy logic and probabilistic logic theory. *International Journal of Advanced Computer Science and Applications (IJACSA)*, 3(12):164–173, 2013.

[94] Canh Ngo, Peter Membrey, Yuri Demchenko, and Cees de Laat. Policy and context management in dynamically provisioned access control service for virtualized cloud infrastructures. In *2012 Seventh International Conference on Availability, Reliability and Security*, pages 343–349, 2012.

[95] Michele Nitti, Roberto Girau, and Luigi Atzori. Trustworthiness management in the social internet of things. *IEEE Transactions on Knowledge and Data Engineering*, 26(5):1, 2013.

[96] Ralf Nyrén and et al. Open cloud computing interface - core. Specification GFD-P-R.183, OCCI-WG, 2011.

[97] OpenStack. Open source cloud computing software. http://openstack.org, 2011.

[98] Jaehong Park and Ravi Sandhu. The ucon abc usage control model. *ACM Transactions on Information and System Security*, 7:128–174, 2004.

[99] Donn B. Parker. *Fighting computer crime: a new framework for protecting information.* John Wiley & Sons, Inc., New York, NY, USA, 1998.

[100] Juan M. Marun Perez, Jorge Bernal Bernabe, Jose M. Alcaraz-Calero, Felix J. Garcia Clemente, Gregorio Martinez Perez, and Antonio F. Gomez Skarmeta. Semantic-aware authorization architecture for grid security. *Future Generation Computer Systems*, 27:40–55, 2011.

[101] Dana Petcu, Beniamino Di Martino, Salvatore Venticinque, Massimiliano Rak, Tamas Mahr, Gorka Esnal Lopez, Fabrice Brito, Roberto Cossu, Miha Stopar, Svatopluk perka, and Vlado Stankovski. Experiences in building a mosaic of clouds. *Journal of Cloud Computing: Advances, Systems and Applications*, 2(1):12, 2013.

[102] Juan Rada-Vilela. fuzzylite: a fuzzy logic control library, 2014.

[103] E Rescola and N Modadugu. Rfc 4347: Datagram transport layer security (dtls). *Request for Comments, IETF*, 2006.

[104] B.P. Rimal, Eunmi Choi, and I. Lumb. A taxonomy and survey of cloud computing systems. In *INC, IMS and IDC, 2009. NCM '09. Fifth International Joint Conference on*, pages 44–51, 2009.

[105] E Rissanen. extensible access control markup language (xacml) version 3.0 oasis standard, 2012.

[106] Hans Schaffers, Nicos Komninos, Marc Pallot, Brigitte Trousse, Michael Nilsson, and Alvaro Oliveira. *Smart cities and the future internet: Towards cooperation frameworks for open innovation.* Springer, 2011.

[107] L. Seitz and G. Selander. Problem description for authorization in constrained environments. *IETF Internet Draft, draft-seitz-ace-problem-description-01*, 2014.

[108] Z. Shelby, K. Hartke, and C. Bormann. The constrained application protocol (coap). *IETF RFC 7252*, 10, June 2014.

[109] Evren Sirin, Bijan Parsia, Bernardo Cuenca Grau, Aditya Kalyanpur, and Yarden Katz. Pellet: A practical OWL-DL reasoner. *Journal of Web Semantics*, 5(2):51 – 53, 2007.

[110] Avvari Sirisha and G. Geetha Kumari. Api access control in cloud using the role based access control model. In IEEE, editor, *Trendz in Information Sciences & Computing*, pages 135–137. IEEE, IEEE, 2010.

[111] Mathias Slawik, Tatiana Ermakova, Jonas Repschläger, Axel Küpper, and Rüdiger Zarnekow. Securing medical saas solutions using a novel end-to-end encryption protocol. In *22st European Conference on Information Systems, ECIS 2014, Tel Aviv, Israel, June 9-11, 2014*, 2014.

[112] Stelios Sotiriadis, Euripides GM Petrakis, Stefan Covaci, Paolo Zampognaro, Eleni Georga, and Christoph Thuemmler. An architecture for designing future internet (fi) applications in sensitive domains: Expressing the software to data paradigm by utilizing hybrid cloud technology. In *Bioinformatics and Bioengineering (BIBE), 2013 IEEE 13th International Conference on*, pages 1–6. IEEE, 2013.

[113] S. Subashini and V. Kavitha. A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications*, 34(1):1 – 11, 2011.

[114] Jin Taige and Qin Xiaolin. A trustworthiness-based access control model in grid system. In *International Conference on Computational Intelligence and Software Engineering CiSE 2009*, pages 1–6, 2009.

[115] H. Takabi, J.B.D. Joshi, and Gail-Joon Ahn. Securecloud: Towards a comprehensive security framework for cloud computing environments. In *Computer Software and Applications Conference Workshops (COMPSACW), 2010 IEEE 34th Annual*, pages 393–398, 2010.

[116] Takeshi Takahashi, Youki Kadobayashi, and Hiroyuki Fujiwara. Ontological approach toward cybersecurity in cloud computing. In *Proceedings of the 3rd international conference on Security of information and networks*, SIN '10, pages 100–109, New York, NY, USA, 2010. ACM.

[117] Huu Tran, Paul Watters, Michael Hitchens, and Vijay Varadharajan. Trust and authorization in the grid: A recommendation model. In IEEE, editor, *Proceedings. International Conference on Pervasive Services*, pages 433 – 436, 2005.

[118] Wei-Tek Tsai and Qihong Shao. Role-based access-control using reference ontology in clouds. In *Proceedings 2011 10th International Symposium on Autonomous Decentralized Systems ISADS 2011*, volume 2, pages 121–128. Ieee, 2011.

[119] Dmitry Tsarkov and Ian Horrocks. *Automated Reasoning*, volume 4130 of *Springer Lecture Notes in Computer Science*, chapter FaCT++ Description Logic Reasoner: System Description, pages 292–297. Springer Berlin / Heidelberg, 2006.

[120] Vlasios Tsiatsis, Alexander Gluhak, Tim Bauge, Frederic Montagut, Jesus Bernat, Martin Bauer, Claudia Villalonga, Payam M Barnaghi, and Srdjan Krco. The sensei real world internet architecture. In *Future Internet Assembly*, pages 247–256, 2010.

[121] University of Murcia. Complete definition of sofic ontology. [Online]. Available: http://reclamo.inf.um.es/sofic, 2014.

[122] LuisM. Vaquero, Luis Rodero-Merino, and Daniel Morán. Locking the sky: a survey on iaas cloud security. *Computing*, 91(1):93–118, 2011.

[123] Thomas Vetterli, Anca Vaduva, and Martin Staudt. Metadata standards for data warehousing: Open information model vs. common warehouse metadata. *ACM SIGMOD Record*, 29(3):68 – 75, 2000.

[124] W. Viriyasitavat and A. Martin. A survey of trust in workflows and relevant contexts. *Communications Surveys Tutorials, IEEE*, PP(99):1 –30, 2011.

[125] V.Vijayakumar and R.S.D.Wahida Banu. Security for resource selection in grid computing based on trust and reputation responsiveness. *International Journal of Computer Science and Network Security*, 8(11):107 – 105, 2008.

[126] Shouxin Wang, Li Zhang, Na Ma, and Shuai Wang. An evaluation approach of subjective trust based on cloud model. *Transform*, 21:1062–1068, 2008.

[127] Mark Weiser. The computer for the 21st century. *Scientific american*, 265(3):94–104, 1991.

[128] ZHU Xiao-jun, LV Shi-qin, YU Xue-li, and Zuo Guang-Ping. Dynamic authorization of grid based on trust mechanism. In IEEE, editor, *2010 International Symposium on Intelligence Information Processing and Trusted Computing*, pages 417–421, 2010.

[129] Houren Xiong and Bin Zhang. Research on context and trust-based grid service authorization model. In IEEE, editor, *2010 International Conference on Multimedia Information Networking and Security*, pages 433–437, 2010.

[130] Jing Xu, Tang Jinglei, He Dongjian, Zan Linsen, Chen Lin, and Niu Fang. Research and implementation on access control of management-type saas. In IEEE, editor, *The 2nd IEEE International Conference on Information Management and Engineering*, pages 388–392. IEEE, IEEE, April 2010.

[131] Junzhou Luo Xudong Ni. A trust aware access control in service oriented grid environment. In IEEE, editor, *Sixth International Conference on Grid and Cooperative Computing*, pages 1–6, 2007.

[132] Ronald R. Yager and Dimitar Filev. *Essentials of fuzzy modeling and control.* Wiley, 1994.

[133] Ran Yang, Chuang Lin, Yixin Jiang, and Xiaowen Chu. Trust based access control in infrastructure-centric environment. In IEEE, editor, *IEEE International Conference on Communications (ICC)*, pages 1–5, 2011.

[134] Sami Yangui, Iain-James Marshall, Jean-Pierre Laisne, and Samir Tata. Compatibleone: The open source cloud broker. *Journal of Grid Computing*, 12(1):93–109, 2014.

[135] L. Youseff, M. Butrico, and D. Da Silva. Toward a unified ontology of cloud computing. In *Grid Computing Environments Workshop, 2008. GCE '08*, pages 1–10, 2008.

[136] E. Yuan and J. Tong. Attributed based access control (ABAC) for web services. In *Proc. of the 12th IEEE International Conference on Web Services (ICWS), Orlando, USA*. IEEE, July 2005.

[137] Tiezhu Zhao and Shoubin Dong. A trust aware grid access control architecture based on abac. In *2010 Fifth IEEE International Conference on Networking, Architecture, and Storage*, pages 1–6, 2010.

[138] Sébastien Ziegler, Cedric Crettaz, Latif Ladid, Srdjan Krco, Boris Pokric, Antonio F Skarmeta, Antonio Jara, Wolfgang Kastner, and Markus Jung. *Iot6–moving to an ipv6-based future iot.* Springer Berlin Heidelber, 2013.