کارگاه های آموزشی مرکز اطلاعات علمی جهاد دانشگاهی

کارگاه آنلاین آشنایی با پایگاه های اطلاعات علمی
بین المللی و
ترفند های جستجو

کارگاه آنلاین
روش تحقیق و مقاله نویسی علوم انسانی

کارگاه آنلاین
پرپوزال نویسی و پایان نامه نویسی

سیزدهمین کنفرانس ملی انجمن کامپیوتر ایران
جزیره کیش، خلیج فارس، ایران
۱۹ الی ۲۱ اسفند ۱۳۸۶
پوستر

کنترل دسترسي حافظ حريم خصوصي در محيطهاي پويا و باز با استفاده از مفهوم اعتماد

مهرنوش شاکرمي
دانشجوي کارشناسي ارشد نرم افزار،
دانشکده مهندسي کامپيوتر، دانشگاه صنعتي شريف،تهران، ايران
shakaramy@ce.sharif.edu

سمانه عباسی مقدم
دانشجوي کارشناسي ارشد نرم افزار،
دانشکده مهندسي کامپيوتر، دانشگاه صنعتي شريف،تهران، ايران
s_moghaddam@ce.sharif.edu

چکيده

سيستم هاي قديمي کنترل بر اساس قواعدي عمل مي‌نمايند که بر اساس مشخصات و اطلاعات شخصي افراد صورت مي‌گيرد. اين اطلاعات که در دسترس فراهم‌کنندگان سرويس قرار مي‌گيرد، مي‌تواند باعث نقض حريم خصوصي افراد شود؛ به‌همين دليل به سيستم هاي کنترل دسترسي روي مي‌آوريم که به مسئله حريم خصوصي افراد توجه کنند. در اين پژوهش يک دسته‌بندي کلي از اين روش‌ها ارائه شده و سپس با ارائه يکي از جديدترين اين روش‌ها، راهکارهاي جديدي را براي تکميل و ترکيب آن با استفاده از مفهوم اعتماد پيشنهاد نموده ايم.

کلمات کليدي

کنترل دسترسي، حريم خصوصي، سياست‌هاي پويا، اعتماد

1- مقدمه

افزايش روزافزون نقش سرويس‌هاي الکترونيکي و اتکا به شبکه‌هاي کامپيوتري، دنياي امروز را به دنياي دانش الکترونيکي تبديل کرده است. به موازات فراگير شدن اين پيشرفت‌ها، حفاظت از داده‌هاي محرمانه و حاوي اطلاعات حساس به نگراني مهمي تبديل شده است.

براي ساختن يک زيرساخت ارتباطي يکپارچه، فراگير و قابل اعتماد به ايجاد مدل‌هاي جديد کنترل دسترسي نيازمنديم و در اين راستا به راهبردهاي "کنترل دسترسي با حفظ حريم خصوصي"[1] روي مي‌آوريم که دو مفهوم "کنترل دسترسي"[2] و "حريم خصوصي"[3] را در يک چارچوب همگن با يکديگر ترکيب مي‌کنند.

در اين مقاله، مروري بر روش‌هاي موجود براي حفظ حريم خصوصي ارائه شده است. سپس اين روش‌ها را از ديدگاه‌هاي مختلف دسته‌بندي نموده ايم. سپس با استفاده از مفهوم اعتماد با استفاده از اسناد RDF[4] راهکار جديدي را پيشنهاد نموده ايم که براي محيط‌هاي پويا و باز به خوبي نياز به حفظ حريم خصوصي را برآورده مي‌سازد.

سازماندهي ساير بخش‌هاي مقاله به اين‌ترتيب است: در بخش 2، مرور مختصري بر تلاش‌هايي که تاکنون در اين زمينه انجام شده است، در بخش 3 يک دسته‌بندي کلي از روش‌هاي موجود آمده است. يک سيستم کنترل پويا‌ي دسترسي حافظ حريم خصوصي در بخش 4 تشريح شده است. در بخش 5 راهکارهاي جديدي براي توسعه آن و سيستم جديد پيشنهادي در بخش 6 آمده است. نتيجه‌گيري و چشم‌اندازي از کارهاي آينده را در بخش 7 مطرح نموده ايم.

2- کارهاي مربوطه

يکي از زمينه‌هايي که مساله حفظ حريم خصوصي در آن مطرح مي‌شود، کاربردهاي مبتني بر مکان است.

Myles و همکارانش [1] معماري را ارائه داده‌اند که در آن يک سرور مکاني وجود دارد که دسترسي‌هاي سرويس گيرندگان را از طريق يک ماژول اعتبارسنجي چک مي‌کند.

XACML[5] [2] يک زبان مبتني بر XML است که براي تعريف سياست‌هاي کنترل دسترسي به‌کار مي‌رود.

از کارهاي برجسته در زمينه کنترل دسترسي با حفظ حريم خصوصي، پروژه PRIME[6] [3] است.

Ardagna و همکارانش در [4] يک معماري براي مولفه نرم‌افزاري تابع تصميم‌گيري کنترل دسترسي ارائه داده‌اند.

Cheung و Gil [5] روشي ارائه کرده‌اند که در آن از DAML-S، RDF و تعريف آنتولوژي‌هاي زمينه‌اي بهره جسته‌اند.

همچنين در راستاي تحقيقات HP در زمينه حريم خصوصي، Pearson و Mont در [6]، سيستمي براي اعمال سياست‌هاي تخصيص منابع در محيط‌هاي پويا ارائه کرده‌اند.

3- دسته بندي كارهاي پيشين

دسته‌بندي تلاش‌هاي انجام شده در اين زمينه از ديدگاه‌هاي مختلفي قابل انجام است.

3-1- دسته‌بندي بر اساس مبناي اعطاي دسترسي

از ديدگاه مبناي اعطاي دسترسي اين روش‌ها را به دو دسته تقسيم مي‌نماييم.

3-1-1- روش‌هاي كنترل دسترسي حافظ حريم خصوصي مبتني برخصوصيت

ايده اصلي اين روش‌ها، اتكا به اعتبارنامه‌هاي ديجيتالي است كه براي زيرساخت‌هاي ارتباطي در محيط‌هاي باز بسيار مناسبتر از شناسه‌ها هستند.

3-1-2- روش‌هاي كنترل دسترسي حافظ حريم خصوصي آگاه از معنا

در اين روش‌ها، اعمال سياست‌هاي كنترل دسترسي حافظ حريم خصوصي با آگاهي از معنا و اغلب با استفاده از تكنيك‌هاي موجود در وب معنايي صورت مي‌گيرد. در اين روش‌ها يك مدلسازي معنايي از اطلاعات محرمانه صورت مي‌گيرد كه به كاربران اجازه كنترل كردن افشاي داده‌ها متناسب با نيازهاي امنيتي خود را مي‌دهد و براي مديران سيستم نيز امكان تعيين انعطاف‌پذيراطلاعاتي كه براي دستيابي به يك سرويس يا داده مورد نياز است را فراهم مي‌نمايد.

3-2- دسته‌بندي بر اساس موجوديت محافظت شونده

در اين روش‌ها مالك اطلاعات حساس، مبناي دسته‌بندي‌ها است. بر اين اساس دو دسته كلي از روش‌ها تشخيص داده مي‌شود:

3-2-1- حفظ حريم خصوصي كاربران

در اين دسته، حفظ حريم خصوصي كاربران سيستم مد نظر است.

3-2-2- حفظ حريم خصوصي سرورها

در دسته دوم، حفظ حريم خصوصي تامين‌كنندگان خدمات مهم است.

3-3- دسته‌بندي بر اساس داده يا پردازش

از اين ديدگاه، روش‌ها را به دو دسته تقسيم مي‌كنيم.

3-3-1- روش‌هاي حفاظت از داده

هدف در اين دسته از روش‌ها، حفاظت از منابع داده‌اي و محصولات داده‌اي توليدشده در حين روند تحليل داده است.

3-3-2- روش‌هاي حفاظت از پردازش

هدف اصلي در اين دسته از روش‌ها حفاظت از دانشي است كه در پروسه‌هاي تحليل داده به دست آمده است.

3-4-دسته‌بندي بر اساس خصوصيت مورد حفاظت داده

بر اين اساس سياست‌هاي كنترل دسترسي مي‌توانند مكان درخواست‌دهنده، پردازشي كه قرار است پس از افشاي داده روي آن صورت بگيرد و يا ساير ملاك‌ها باشد.

4- سيستم تخصيص منابع و پردازش داده‌ي آگاه از حريم خصوصي در محيط-هاي پويا

4-1- معرفي مساله

موسسات مختلف مقادير زيادي داده محرمانه درباره كارمندان، مشتريان و شركاي خود ذخيره مي‌كنند. از طرفي، دستيابي و مديريت اين داده‌ها براي اين موسسات ضروري است.

4-2- مدل كلي سيستم ارائه شده

هدف ارائه يك سيستم مديريت حريم خصوصي است كه سياست‌هاي مربوط به آن به شكل پويا و بر اساس زمينه جاري تعيين مي-شوند. اين راه‌حل شامل مكانيزم‌هاي تامين‌كننده موارد زير است:

- مشخص كردن محدوديت‌ها براي تخصيص پوياي منابع بر اساس سياست‌هاي حفظ حريم خصوصي.
- انتخاب پوياي منابع بر اساس چك كردن سياست‌هاي مشخص شده در بسته سياست‌ها، در مقابل خصوصيات كنوني منابع و درخواست‌كننده.
- اعمال و افشاي سياست‌هاي مذكور با نظارت يك سرويس معتمد حريم خصوصي[7]
- تعيين مكان منابع به شكل قابل اعتماد

در واقع اين سيستم سعي دارد هر دو نياز زير در برآورده نمايد:

- حصول اطمینان از اینکه درخواست-دهنده داده بر اساس اطلاعاتي كه از زمینه خود مي‌دهد و سیاست‌هاي موجود، صلاحیت دسترسي به داده حساس را دارد.
- حصول اطمینان از صحت اطلاعاتي كه درخواست‌دهنده راجع به زمینه كاري خود به ما مي‌دهد.

هر منبع با یک یا چند TPS در تعامل است تا بتواند به محتویات داده‌هاي محرمانه مخفي شده دست یابد. از طرف دیگر، روي هر منبع یک گزارش‌دهنده معتمد مكان[8] نصب شده است كه اطلاعات مربوط به مكان منبع را در دسترس TPS قرار مي‌دهد.

در بخش‌هاي بعد شرح مختصري از هر یک از اجزاي مدل را آورده‌ایم.

4-3- بسته سیاست‌ها

در این بسته، مجموعه‌اي از سیاست‌هاي مرتبط با زمینه كه شرایط، وظایف و نیازمندي‌ها را لحاظ مي‌كنند؛ به همراه یکسري متاسیاست‌ها براي انتخاب سیاست قابل اعمال موجود است.

4-4- سرویس معتمد حریم خصوصي

سرویس معتمد حریم خصوصي، یک وب‌سرویس مطمئن و قابل اعتماد است كه سازگاري با سیاست‌ها را چک مي‌كند.

در این روش، منابع شامل یک ماژول براي دسترسي به این سرویس هستند كه به عنوان یک عامل نصب شده محلي[9] عمل مي-كند.

این سرویس و ماژول دسترسي آن داراي یک "موتور سیاست"[10] براي تفسیر سیاست‌ها هستند.

4-5- گزارش‌دهنده معتمد مكان

این بخش در واقع اطلاعات مربوط به مكان منابع را تامین مي‌كند و داراي دو جزء كلیدي است:

- یک لایه نرم‌افزاري قابل اعتماد براي تعیین یا تایید محل منبع از طریق یک API
- یک سري اجزاي مطمئن كه مي‌تواند اطلاعات مكاني دقیق‌تري به ما بدهد.

5- راهكار جدید ارائه شده براي توسعه و فراگیرتر شدن روش

5-1- ترکیب نظریات Trust و Privacy

ایده اصلي در این بخش، ترکیب نظریات مربوط به "اعتماد"[11] با سیاست‌هاي كنترل دسترسي حافظ منابع شخصي است. ابتدا به معرفي مفهوم "اعتماد" مي‌پردازیم.

5-1-1- مفهوم اعتماد

منظور ما از اعتماد در این مقاله میزان اعتمادي است كه كاربر یا به طور كلي‌تر مالک داده‌هاي محرمانه، به میزان صلاحیت عامل درخواست‌دهنده داده-ها دارد.

از آنجا كه این سیستم مي‌تواند در محیط‌هاي ارتباطي باز مانند اینترنت استفاده شود، مي‌توان اعتماد را در معناي دیگري كه امروزه در وب معنایي متداول است با مفهوم حریم خصوصي ترکیب نمود. در این حالت، مي‌توان از "اعتماد بر مبناي شهرت"[12] كه به معناي میزان اعتماد به یک عامل بر اساس سوابق عملكرد آن در گذشته است و یا "مدل‌هاي عمومي اعتماد"[13] كه میزان اعتماد قابل اندازه‌گیري یک عامل به عامل دیگر را براي دوره مشخصي در ارتباط با یک سرویس معین بیان مي‌كند، بهره گرفت[8].

5-1-2- توسعه سیستم با استفاده از مفهوم اعتماد

با استفاده از مفاهیم بیان شده براي اعتماد، آنچه باید به سیستم پیشین افزوده شود به قرار زیر است:

- توسعه TPS

به TPS یک بخش به نام "عنصر چک‌كننده اعتماد"[14] (TCE) اضافه مي‌كنیم كه مورداعتماد بودن یا نبودن عامل موردنظر را كه به پیش‌شرط‌هاي موجود در سیاست‌هاي بسته سیاست‌ها اضافه شده است را چک كند.

- توسعه بسته سیاست‌ها

در این توسعه، مي‌توان ارائه یکسري گواهي‌نامه‌هاي اعتباري(در مورد اعتماد مبني بر سیاست) و یا تامین میزان مطلوبي از اعتماد(در مورد مفهوم دوم مطرح شده براي اعتماد) را جزو پیش‌شرط-هاي بیان شده در سیاست‌ها در نظر گرفت.

- افزودن بخشي به نام "تامین‌كننده قابل اعتماد اعتبارنامه"[15] (TCP)

در حالتي كه اعتماد مبتني بر سیاست‌ها مورد نظر است كه براي آن باید یکسري گواهي‌ها ارائه شود، این بخش به هر منبع اضافه مي‌شود.

- لیستي از منابع قابل اعتماد[16] (TRL)

در حالتي كه از معناي اعتماد براي محیط-هاي باز استفاده مي‌نماییم، این لیست در هر منبع نگه‌داري مي‌شود. زماني كه

داده محرمانه به سایر منابع فرستاده می‌شود این لیست نیز به همراه داده محرمانه رمز می‌شود.

6- ارائه سیستم جدید پیشنهادی با استفاده از RDF Trust

در این بخش برای تکمیل سیستم ارائه شده در بخش 5، از توسعه یاد شده در بخش پیشین بهره می‌جوییم.

فرض می‌کنیم که به همراه هر داده محرمانه رمز شده، اطلاعات مربوط به آن به صورت RDF فرستاده شده است.

درون هر منبع داده لیستی از سایر منابع شبکه به همراه میزان اعتمادی که این منبع به هر یک از آنها دارد، موجود است. این لیست Bookmark نامیده می‌شود.

برای رسیدن به این منظور، صفات RDF جدیدی بیان می‌شوند تا با استفاده از آنها RDF Trust بیان شود.

- افزودن صفت bookmark:retrivedFrom

این صفت، مشخص کننده URI مالک داده محرمانه است.

- افزودن صفت bookmark:prefer

این صفت برای هر منبع موجود در شبکه، وزن اعتمادی را مشخص می‌کند که منبع دارنده Bookmark برای آن در نظر گرفته است.

وقتی بسته سیاست‌ها در TPS بررسی می‌شود به ترتیب زیر عمل می‌شود:

با توجه به Reification موجود به همراه داده محرمانه، URI مالک آن پیدا می‌شود و سپس با رجوع به RDF Bookmark آن منبع و با استفاده از صفت bookmark:prefer مشخص می‌شود که مالک داده محرمانه تا چه حد به درخواست‌دهنده اعتماد دارد. از روی مقدار این صفت و با توجه به سیاست‌های مشخص شده در بسته سیاست‌ها، TPS می‌تواند راجع به صدور تصمیم درست کنترل دسترسی اقدام نماید.

7- نتیجه‌گیری و کارهای آینده

در این مقاله ضمن معرفی عرصه جدید کنترل دسترسی با حفظ حریم خصوصی و دسته‌بندی روش‌های موجود، روش جدیدی ارائه شد که مفاهیم وب معنایی مانند اعتماد را با یک سیستم کنترل دسترسی موجود ترکیب می‌کند. در پژوهش‌های آتی سعی داریم نمونه‌های دیگری از روش‌های اعمال اعتماد را در تصمیم‌گیری‌های کنترل دسترسی حافظ حریم خصوصی، لحاظ نماییم.

8- مراجع

[1] Ginger Myles, Adrian Friday, and Nigel Davies: *Preserving Privacy in Environments with Location-Based Applications*, IEEE Pervasive Computing, 2(1):56–64, 2003.

[2] XACML - (eXtensible Access Control Markup Language), http://www.oasis-open.org/committees/tc\home.php?wg\ abbrev=xacml\#XACML20.

[3] http://ww.prime-project.eu.org

[4] Claudio A. Ardagna, Marco Cremonini, Ernesto Damiani, Sabrina De Capitani di Vimercati and Pierangela Samarati: *The Architecture of a Privacy-aware Access Control Decision Component*, 2005.

[5] William K. Cheung, Yolanda Gil: *Towards Privacy Aware Data Analysis Workflows for e-Science*, Workshop on Semantic e-Science (SeS2007) in conjunction with the Twenty-Second Conference of the Association for the Advancement of Artificial Intelligence (AAAI), Vancouver, Canada, July 23, 2007.

[6] Siani Pearson, Marco Casassa Mont: *A System for Privacy-Aware Resource Allocation and Data Processing in Dynamic Environments*, Trusted Systems Laboratory, HP Laboratories Bristol, March 28, 2007.

[7] Marco Casassa Mont, Robert Thyne: *Privacy Management for Governance*, RSA Conference 2005.

[8] Donovan Artz and Yolanda Gil: *A Survey of Trust in Computer Science and the Semantic Web*, To appear in Journal of Web Semantics: Science, Services and Agents on the World Wide Web, 2007.

زیرنویس‌ها

[1] privacy aware access control
[2] access control
[3] privacy
[4] Resource Description Format
[5] eXtensible Access Control Markup Language
[6] Privacy and Identity Management for Europe
[7] TPS : Trusted Privacy Service
[8] TLP : Trusted Localisation Provider
[9] locally installed agent
[10] policy engine
[11] Trust
[12] Reputation-based trust
[13] General models of trust
[14] TCE : Trust Checking Element
[15] TCP : Trusted Certificate Provider
[16] TRL : Trusted Resources' List

کارگاه های آموزشی مرکز اطلاعات علمی جهاد دانشگاهی

کارگاه آنلاین آشنایی با پایگاه های اطلاعات علمی بین المللی و ترفند های جستجو

کارگاه آنلاین
روش تحقیق و مقاله نویسی علوم انسانی

کارگاه آنلاین
پروپوزال نویسی و پایان نامه نویسی