پنجمین کنفرانس انجمن رمز ایران
انجمن رمز ایران
Iranian Society of Cryptology
۲۴ الی ۲۶ مهر ماه ۱۳۸۶ دانشگاه علم و صنعت ایران

یک مدل اعتمادِ مبتنی بر هستان‌شناسی و آگاه از معنا برای محیط‌های محاسبات فراگیر

محسن طاهریان
دانشکده مهندسی کامپیوتر
دانشگاه صنعتی شریف
taherian@ce.sharif.edu

مرتضی امینی
دانشکده مهندسی کامپیوتر
دانشگاه صنعتی شریف
m_amini@ce.sharif.edu

رسول جلیلی
دانشکده مهندسی کامپیوتر
دانشگاه صنعتی شریف
jalili@sharif.edu

چکیده: به طور معمول، کامپیوترهای تنها و شبکه‌های کوچک به منظور تأمین امنیت، به احراز اصالت کاربر و مکانیزم‌های کنترل دسترسی تکیه می‌کنند. اما این روش‌ها برای به‌کارگیری در محیط‌های توزیع‌شده نظیر اینترنت و محیط‌های محاسبات فراگیر با مشکل عدم انعطاف‌پذیری و عدم گسترش‌پذیری مواجه هستند، زیرا که این محیط‌ها فاقد یک کنترل‌کننده مرکزی هستند و تمامی کاربران آنها نیز از پیش مشخص نیست. بدست آوردن میزان اعتماد عناصر و افراد به یکدیگر و اتخاذ تصمیم‌های امنیتی با کمک این مقادیر می‌تواند نقش مهمی در افزایش امنیت این‌گونه محیط‌ها ایفا کند. تا کنون مدل‌های متعددی برای اعتماد در محیط‌های محاسبات فراگیر ارائه شده است ولی هنوز مدلی که بتواند روابط معنایی میان عناصر این محیط‌ها را به طور کامل بپوشاند، مطرح نگردیده است. ما با استفاده از مفهوم هستان‌شناسی که در وب‌معنایی وجود دارد، یک مدل اعتماد برای محیط‌های محاسبات فراگیر ارائه کرده‌ایم که قادر است روابط معنایی میان ابزارهای فراگیر و همچنین رسته‌های اعتماد را در خود بگنجاند و در ضمن با استفاده از این روابط و تعاملات میان ابزارها، میزان اعتماد عناصر به یکدیگر را محاسبه کند و در تصمیم‌گیری‌های امنیتی لحاظ کند. استفاده از ساختار هستان‌شناسی به ما امکان افزودن مفاهیم مهم دیگری نظیر مفهوم زمینه در محیط‌های فراگیر را به مدل فراهم می‌کند.

واژه های کلیدی: محیط‌های محاسبات فراگیر، مدل اعتماد، وب‌معنایی، هستان‌شناسی، رسته‌های اعتماد، زمینه.

۱- مقدمه

امروزه با گسترش روز افزون حجم داده‌ها و در نتیجه پیشروی به سمت توزیع‌شدگی داده‌ها، یکی از مسائلی که بسیار مورد توجه قرار گرفته است، حفظ امنیت کاربران و داده‌هاست. با بوجود آمدن سیستم‌های توزیع‌شده، کارهای بسیاری در مورد جنبه‌های مختلف امنیت این سیستمها شکل گرفت و پیشرفت‌های زیادی نیز حاصل گردید. ولی با گذشت زمان و افزایش میزان توزیع‌شدگی محیط‌های اطلاعاتی، تطبیق الگوریتم‌های مطرح‌شدهِ توزیع‌شده با چالش-های جدید در این محیطها کاری سخت و پیچیده گشت و

تحقیقات نشان داد که به‌کارگیری مکانیزم‌های کنترل دسترسی قدیمی دیگر پاسخگوی نیازهای جدید کاربران نیستند [1,2]. یکی از مسائلی که مکانیزم‌های قدیمی امنیتی آن را در نظر نمی‌گیرند، مساله اعتمادی است که در دنیای واقعی و در بخش‌های مختلفی از زندگی اجتماعی، میان انسانها با خود و یا عوامل محیط شکل می‌گیرد [3]. در واقع بسیاری از مسائل مطرح شده در محیطهای توزیع‌شده‌ای نظیر تبادلات، و خرید و فروش الکترونیکی را می‌توان با یک سیستم رأی‌دهی و امتیازدهی ساده که از اعتقاد طرفین نتیجه می‌شود، برطرف نمود.

یکی از انواع محیطهای توزیع‌شده‌ای که از سال ۱۹۹۱ و با نگاهی جدید به آینده محیطهای محاسباتی و اطلاعاتی پدید آمد، محیط محاسبات فراگیر[1] است. در این محیطها سعی می‌شود، کامپیوترها به پس‌زمینه برده شوند و آنها را چنان در محیط اطراف زندگی تعبیه کنند که در عین اینکه کاملا در دسترس و قابل استفاده‌اند، از دید افراد پنهان باشند [4]. همانطور که گفته شد، با توجه به عدم کاربردپذیری مناسب روشهای امنیتی قدیمی در اینگونه محیطها، ارائه یک مدل اعتماد برای محیطهای فراگیر از مسائلی است که امروزه مورد توجه محققین قرار گرفته است.

تا کنون مدلهای اعتماد زیادی برای محیطهای توزیع‌شده‌ای نظیر شبکه‌های اجتماعی مبتنی بر وب [5,6] و شبکه‌های همتا-همتا (P2P) [7] و محاسبات فراگیر ارائه شده اند که هر یک به طریقی سعی در افزایش امنیت این گونه محیطها داشته‌اند. استفاده از هستان‌شناسی برای بیان روابط معنایی میان عناصر فراگیر قبلا نیز مطرح شده است و سعی شده است مانند بسیاری از حوزه‌های دیگر، یک هستان‌شناسی استاندارد برای آن طراحی شود. هستان‌شناسی SOUPA به این منظور درنظر گرفته شده است [8,9]. ولی مسأله مهمی که تا کنون به طور خاص در مورد محیطهای محاسبات فراگیر به آن پرداخته نشده است، نقش روابط معنایی میان عناصر فراگیر در برقراری اعتماد میان آنها است. در این مقاله، مدلی جدید از اعتماد در محیط محاسبات فراگیر بر پایه مفاهیم موجود در وب‌معنایی ارائه شده است که به خوبی با الهام گرفتن از ساختار هستان‌شناسی[2] می‌تواند روابط معنایی و سلسله‌مراتبی میان عناصر و رسته‌های اعتماد[3] را بپوشاند. علاوه بر این، استفاده از هستان‌شناسی به ما امکان می‌دهد که مفاهیم مهمی در محاسبات فراگیر نظیر «زمینه» را به سادگی به مدل اضافه کنیم.

در این مدل روابط اعتماد میان عناصر با یک زبان رسمی بیان می‌شود و بر اساس امتیازدهی عناصر به یکدیگر پس از انجام یک تعامل، امکان محاسبه مقدار جدید اعتماد و به روز رسانی آن نیز فراهم می‌گردد. هر عنصر می‌تواند بر اساس خط‌مشی‌های امنیتی خود و بر اساس میزان اعتماد خود، تصمیم به برقراری ارتباط با موجودیت‌های دیگر بگیرد.

در ادامه مقاله، در بخش بعد، کارهای مرتبط و مدلهای اعتماد ارائه شده تا کنون برای محیطهای محاسبات فراگیر مورد بررسی و مرور قرار می‌گیرند. در بخش ۳، مدل پیشنهادی بر اساس ساختارهای هستان‌شناسی به تفصیل ارائه می‌گردد و سپس در بخش ٤ مؤلفه‌های مدل، گردش اطلاعات در مدل و الگوریتمهای استنتاج و ترکیب اعتماد تشریح می‌شوند. در بخش ٥، به ارزیابی مدل پیشنهادی و مقایسه آن با سایر مدل‌های ارائه شده می‌پردازیم و در نهایت، در بخش ٦، یک جمع‌بندی و نتیجه‌گیری از مطالب ذکر شده، ارائه می‌شود و مسیرهای پیش‌رو برای ادامه کار ترسیم می‌گردند.

۲- کارهای مرتبط

در میان مدلهای مختلفی که برای اعتماد در محیطهای توزیع‌شده ارائه شده است،برخی افراد سعی‌کرده‌اند که یک مدل اعتماد کلی ارائه دهند که در همه محیطهای توزیع‌شده کاربرد داشته باشد. معتبرترین این مدلها، کاریست که عبدالرحمان[4] در [10] انجام داده است. با این حال، اکثر مدلها به بررسی اعتماد در یک محیط توزیع‌شده‌ی خاص پرداخته‌اند که ما در این قسمت، چند نمونه از آنها که به طور خاص برای محیط محاسبات فراگیر ارائه شده‌اند، را بررسی می‌کنیم.

[1] Pervasive Computing Environments

[2] Ontology
[3] Trust Categories
[4] A. Abdul-Rahman

یکی از شناخته‌ترین مدل‌های اعتماد که تا کنون برای محیط محاسبات فراگیر ارائه شده است و حتی در سطح وسیعی نیز پیاده‌سازی شده است، مدلی است که توسط آقای آلمِنارز[5] و همکارانش در سال ۲۰۰۴ پیشنهاد شد و به نام PTM[6] شهرت یافت [11,12]. آنها در این مدل با در نظر گرفتن دو نوع اعتماد یعنی اعتماد مستقیم و اعتماد توصیه‌ای، ساختار مدل خود را به دو بخش تقسیم کرده‌اند. یکی، *فضای باور*[7] که به محض ورود یک موجودیت به محیط، به آن موجویت یک مقدار اعتماد اختصاص می‌دهد و در تعامل اول موجودیت با دیگران، این مقدار لحاظ می‌شود. دیگری، *فضای شهود*[8] که با رفتار موجویت در طول زمان، مقادیر اعتماد آن را به روز می‌کند. اپراتور میانگین وزن‌دار برای ترکیب مقادیر استفاده شده است و مقادیر در فضای باور به صورت فازی بیان شده‌اند. همچنین یک پروتکل ارتباطی برای توصیه مقادیر اعتماد به دیگران نیز تعریف شده است که هنگام تعامل، یک موجودیت می‌تواند با ارسال پیام به دیگران در مورد موجودیت طرف تعاملِ خود کسب اطلاع نماید. این مدل در برخی ابزارهای سیار فراگیر نیز پیاده‌سازی شده [13] و در کنار سایر مؤلفه‌های امنیتی، به بالا بردن سطح امنیت ابزارهای فراگیر کمک می‌نماید.

کار دیگری که در زمینه اعتماد در محیط‌های محاسبات فراگیر انجام شده است و بیشتر به یک نوع مدل *کنترل دسترسی گواهی-مبنا*[9] شباهت دارد، توسط خانم کاگال[10] و همکارانش در سال ۲۰۰۱ مطرح شد [1,14] . در این معماری، در هر دامنه یک عامل مسئول تعریف خط‌مشی‌های امنیتی و کنترل آنهاست که *عامل امنیتی*[11] نامیده می‌شود. وقتی یک کاربر خارجی درخواستی برای دریافت یک سرویس می‌نماید، باید از عاملهای دیگر که از نظر عامل امنیتی معتمّد هستند، گواهی دریافت کند و سپس درخواست خود را به همراه گواهی‌های دریافتی به عامل امنیتی بفرستند تا سرویس مورد نظر را بگیرند.

در هر دو مدل گفته شده در بالا و همچنین سایر مدل‌های اعتماد ارائه شده تا کنون در محیط‌های فراگیر، هنوز نقش ارتباط معنایی موجودیت‌ها و همچنین رسته‌های اعتماد در نظر گرفته نشده است. این ارتباط معنایی می‌تواند نقش مؤثری در ایجاد تعامل میان موجودیت‌ها و همچنین دادن مجوز دسترسی به آنها در گرفتن یک سرویس ایفا کند. به عنوان مثال در نظر بگیرید که فرد A در زمینه انتخاب کارگردان خوب به شخص B اعتماد بالایی دارد. یک نتیجه‌ی قابل استنتاج بگیریم که A می‌تواند تا حد زیادی به B در زمینه پیشنهاد فیلم خوب نیز اعتماد کند. در واقع یک ارتباط معنایی میان دو رسته‌ی اعتماد فیلم خوب و بازیگر خوب وجود دارد.

۳- ساختار مدل پیشنهادی

در مدل پیشنهادی، با استفاده از ساختار هستان‌شناسی، می‌خواهیم روابط معنایی میان عناصر محیط فراگیر و همچنین روابط معنایی میان رسته‌های اعتماد را مدل کنیم. با استفاده از این ساختار و خصوصیات هستان‌شناسی، امکان استنتاج اعتماد برای هر موجودیت در مورد موجودیت‌های دیگر فراهم می‌آید. در این بخش، ابتدا مؤلفه‌های موجود در مدل را به طور کلی بیان کرده، سپس به شرح جزئیات آن می‌پردازیم.

۳-۱- هستان‌شناسیِ اعتماد

در این مدل، برای بیان روابط اعتماد میان موجودیت‌ها در محیط فراگیر یک هستان‌شناسی درنظر گرفته می‌شود. هر هستان‌شناسی O از یک مجموعه از کلاس‌ها و یک مجموعه از خصوصیات تشکیل شده است. مجموعه کلاس‌ها با C و مجموعه خصوصیات با P نمایش داده می‌شوند و داریم:

$$O = \{C, P\}$$

که در آن:

$$C = \{Device, Category, TrustValue, DirectTrust, RecTrust, CategoryRelation, RelevanceValue, Time\}$$

و همچنین:

[5] F. Almenarez
[6] Pervasive Trust Management
[7] Belief Space
[8] Evidence Space
[9] Certificate Based Access Control
[10] L. Kagal
[11] Security Agent

$P = \{subClassOf, hasDirectTrust, hasReCtrust, hasTrustValue, trustedDevice, trustedCategory, trustRelated, relatedCategory, hasRelevanceValue, initialTrustValue, updateTime, collaborationNo\}$

در این قسمت به شرح تک تکِ کلاس‌ها و خصوصیاتی که این کلاس‌ها را به هم ارتباط می‌دهند، می‌پردازیم. از آنجا که روابط در هستان‌شناسی تنها روابط دوتایی هستند (میان دو مفرد برقرار می‌شوند)، برای تعریف رابطه میان چند موجودیت و یا افزودن صفت و مقداری به خود رابطه، ناگزیر از الگویی جدید هستیم که در بخش بعد آن را خواهیم دید.

۳-۱-۱- کلاس‌های هستان‌شناسیِ اعتماد

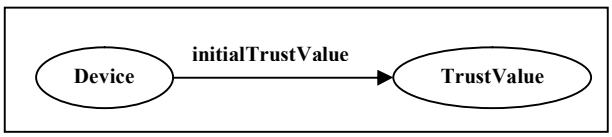
کلاس Device، دربرگیرنده مفردهایی است که بیانگر عناصر و ابزارهای موجود در محیط فراگیر هستند مانند کاربر فراگیر، حسگر، PDA و غیره. از این به بعد، در این مقاله مفردهایی از این نوع کلاس را عنصر *فراگیر* می‌نامیم. کلاس Category مفردهایی را شامل می‌شود که رسته‌های اعتماد را نشان می‌دهند مانند رسته‌ی خواندن از فایل، دادن حق ورود به سیستم و غیره. در واقع رسته‌های اعتماد مشخص کننده‌ی نوع و زمینه‌ی اعتمادی هستند که برای شروع یک دسترسی و یا یک عمل میان دو عنصر فراگیر لازم است. کلاس TrustValue تعیین کننده مقادیر اعتمادی است که به عناصر نسبت داده می‌شود.به عنوان مثال، این مقادیر می‌توانند اعداد اعشاری در بازه [0..1] باشند. کلاس DirectTrust یک کلاس میانی می‌باشد که به ما امکان تعریف رابطه‌ای چند بعدی (با درجه بیشتر از دو) می‌دهد. این کلاس برای تعریف رابطه *اعتماد* مستقیم میان عناصر در نظر گرفته شده است. معنای این رابطه و نحوه تعریف آن را در بخش بعد خواهیم دید. گاهی اوقات در محیط فراگیر یک عنصر به عنصر دیگر باور مستقیمی ندارد (مثل حالتی که تا کنون با آن تعاملی نداشته است). در این حالت ممکن است برای برقراری ارتباط از دیگران نظر بخواهد و با یک الگوریتم استنتاج اعتماد، مقدار اعتماد به آن عنصر را بدست آورد. این مقدار بدست آمده *اعتماد* غیر مستقیم نامیده می‌شود. کلاس RecTrust یک کلاس میانی برای تعریف رابطه اعتماد غیرمستقیم میان عناصر است. یکی از بخش‌های اساسی مدل امکان اتخاذ تصمیم‌گیری‌های امنیتی بر اساس ارتباط و وابستگی میان رسته‌های اعتماد می‌باشد. برای تعریف این رابطه میان رسته‌ها از یک کلاس میانی به نام CategoryRelation استفاده می‌کنیم و مقادیر مجاز برای این وابستگی را در کلاس RelevanceValue مشخص می‌کنیم. در نهایت، کلاس Time نوع و فرمت مقادیری است که برای نمایش زمان از آن استفاده می‌شود. از این کلاس برای بیان زمان بدست آوردن اعتماد در فرآیند استنتاج استفاده می‌شود.

۳-۱-۲- خصوصیاتِ هستان‌شناسیِ اعتماد

در این قسمت، خصوصیات موجود در هستان‌شناسی اعتمادِ مطرح‌شده را شرح می‌دهیم.

- خصوصیت initialTrustValue

یک رابطه از این خصوصیت، به عنصر فراگیر یک مقدار اعتماد اولیه اختصاص می‌دهد. این مقدار، مقداری است که با ورود عنصر جدید به محیط فراگیر، توسط یک عامل به نام *مدیر اعتماد*[۱۲] به آن اختصاص می‌یابد. معیارهای دادن این مقدار به سیاست‌ها و خط‌مشی‌های مدیر اعتماد بستگی دارد. شمای این خصوصیت در شکل ۱ آمده است.



شکل ۱: خصوصیت initialTrustValue

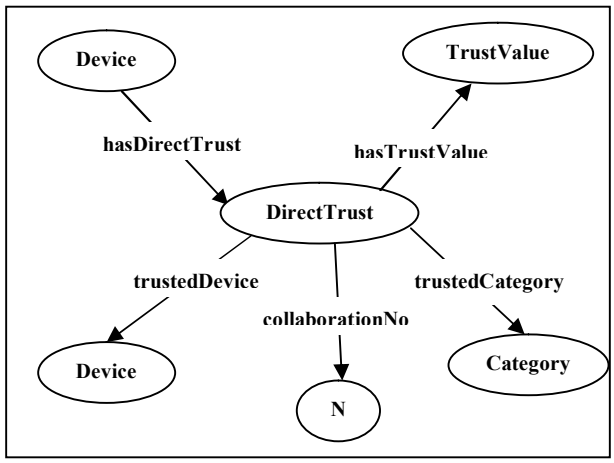
توجه شود که کلاس TrustValue محتوی مقادیری است که اعتماد می‌تواند داشته باشد. در محیط‌های متفاوت این مقدار می‌تواند متفاوت باشد. به عنوان مثال می‌تواند مجموعه اعداد صحیح بین ۱ تا ۱۰ را اتخاذ کند.

- خصوصیت hasDirectTrust

وقتی که یک عنصر با یک عنصر دیگر تعامل می‌کند، میزانی از اعتماد نسبت به آن عنصر بدست می‌آورد. برای بیان این مقدار اعتماد که در واقع یک مقدار اعتماد مستقیم است، رابطه فوق تعریف می‌گردد. این رابطه یک رابطه دوتایی ساده محسوب نمی‌شود. زیرا علاوه بر برقراری ارتباط میان دو عنصر، دارای صفاتی نیز می‌باشد. صفات این رابطه عبارتند از:

[12] Trust Manager

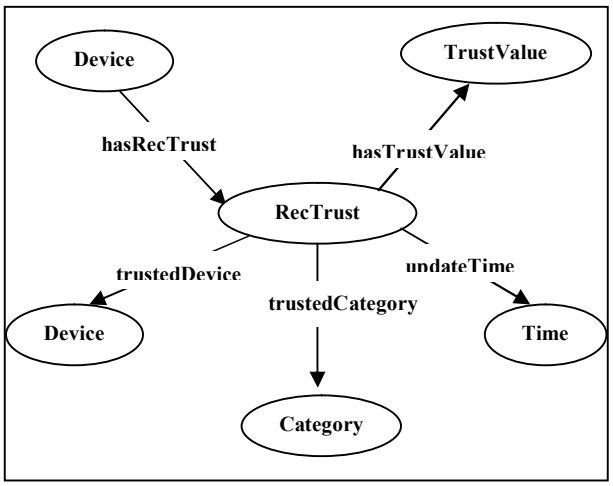
۱) تعداد تعاملات میان آن دو عنصر تا کنون (collaborationNo)، ۲) رسته‌ای که اعتماد در آن رسته شکل گرفته است (Category)، و ۳) مقدار اعتماد (TrustValue). کلاس N که در شکل ۲ دیده می‌شود، مجموعه اعداد طبیعی را شامل می‌شود. برای بیان رابطه‌ای که این صفات را نیز در بر داشته باشد، از ساختار ارائه شده در شکل ۲ استفاده می‌کنیم. توجه شود که کلاس DirectTrust تنها یک کلاس میانی برای افزودن صفات به رابطه می‌باشد.



شکل ۲: خصوصیت hasDirectTrust

- خصوصیت hasRecTrust

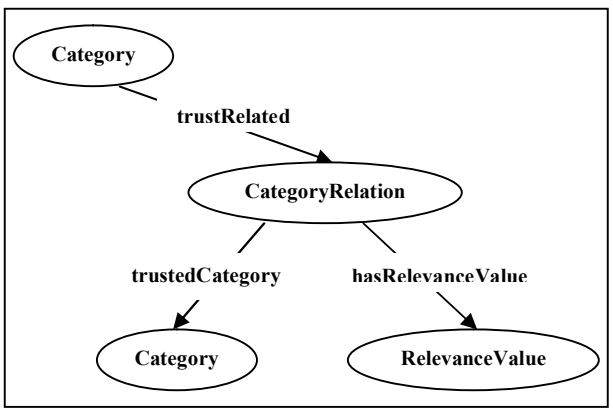
گاهی ممکن است که یک عنصر بخواهد با عنصری که تا کنون با آن تعاملی نداشته است، ارتباط برقرار کند. در این صورت شاید از دیگران بخواهد اعتمادی که به آن عنصر دارند، را در اختیار او قرار دهند. در واقع به این بخش استنتاج اعتماد گفته می‌شود و پس از اجرای رویه استنتاج، مقدار بدست آمده توسط این رابطه درون هستان‌شناسی قرار می‌گیرد. این رابطه هم مانند رابطه hasDirectTrust تعریف می‌شود، با این تفاوت که به جای صفت collaborationNo دارای یک صفت جدید به نام updateTime است. این صفت زمان آخرین استنتاج هر عنصر را در مورد عناصر دیگر نگه می‌دارد. جزئیات رویه استنتاج در بخش ۴ مقاله توضیح داده می‌شود. شمای این خصوصیت در شکل ۳ آمده است.



شکل ۳: خصوصیت hasRecTrust

- خصوصیت trustRelated

ارتباط معنایی موجود میان رسته‌های متفاوتِ اعتماد یکی از خصوصیت‌هایی است که در این مدل در نظر گرفته شده است. مثلا ممکن است میزان اعتماد به یک شخص در زمینه انتخاب یک فیلم، میزانی از اعتماد در زمینه انتخاب کارگردان را نیز به آن فرد نسبت دهد. بنابراین رابطه trustRelated تعریف شده است تا میزان ارتباط رسته‌های اعتماد را مشخص نماید. این رابطه دارای صفت RelevanceValue است که مقدار وابستگی را مشخص می‌کند. شکل ۴ این رابطه را نمایش می‌دهد.



شکل ۴: خصوصیت trustRelated

۳-۲- قوانین امنیتی

یکی از مباحث اصلی در امنیت محیط فراگیر، امن بودن تعامل میان عناصر فراگیر می‌باشد. در محیط فراگیر هر موجودیت برای تعامل خودمختار است و می‌تواند خط‌مشی‌های خاص خود را برای تعامل داشته باشد. این خط‌مشی‌ها به صورت

قوانینی با زبان SWRL[13] بیان می‌شوند که زبانی برای بیان قوانین در OWL می‌باشد. در زیر یک مثال از این قوانین آورده شده است.

فرض کنید که عنصر e_1 می‌خواهد با e_2 ارتباط برقرار کند که نوع این ارتباط در رسته اعتماد c_1 قرار می‌گیرد. یک نمونه قانون در زیر آورده شده است:

$$\begin{aligned} &if \\ &e_2 \ \ isa \ \ Sensor \\ &\quad and \\ &\left[\begin{array}{l} hasDirectTrust(e_1) = X \ \ and \ \ trustedDevice(X) = e_2 \ \ and \\ trustedCategory(X) = c_1 \ \ and \ \ hasTrustValue(X) \geq 0.6 \end{array}\right] \\ &then \ \ collaboration \ \ with \ \ el \ \ in \ \ category \ \ cl \ \ is \ \ granted. \end{aligned}$$

البته در اینجا برای درک بیشتر قانون، به جای زبان SWRL آن را با یک زبان صوری بیان کرده‌ایم. همانطور که دیدیم هر موجودیت هنگام تعامل با دیگران با یک جستجو در هستان-شناسی خود و یافتن قوانین مربوط به آن تعامل، تصمیم به برقراری ارتباط با عنصر دیگر می‌گیرد. توجه شود که با توجه به خط‌مشی‌های امنیتی می‌توان عدم وجود قانون را به معنای عدم اجازه تعامل و یا دادن اجازه تعامل در نظر گرفت.

۴- روش استنتاج اعتماد در مدل

نکته‌ای که هنوز به آن نپرداخته‌ایم پروتکل ارتباطی است که عناصر فراگیر برای بدست آوردن مقدار اعتماد غیرمستقیم بایستی از آن تبعیت کنند و اینکه چگونه مقادیر اعتماد (مستقیم و غیرمستقیم) به روز می‌شوند.

۴-۱- پروتکل استنتاج اعتماد (اعتماد غیرمستقیم)

سادگی پروتکل استنتاج یکی از مسائلی است که با توجه به محدود بودن توان و قدرت ابزار فراگیر در این مدل مورد توجه بوده است. در همان مثال قبل فرض کنید که عنصر e_1 در هستان‌شناسی خود، رابطه hasRecTrust را نداشته باشد و بخواهد از طریق پرسش از دیگران، این رابطه را به هستان-شناسی خود بیفزاید. بنابراین یک پیام به همه موجودیت‌های دیگر پخش همگانی[14] می‌کند. این پیام حاوی یک پرسش به زبان OWL-QL خواهد. شکل این پرسش به همان زبان صوری به شکل زیر است:

$$\begin{aligned} &hasDirectTrust(x) = X \ \ and \ \ trustedDevice(X) = e_2 \ \ and \\ &trustedCategory(X) = c_1 \ \ and \ \ hasTrustValue(X) = ? \end{aligned}$$

بقیه عناصر با گرفتن پیامِ پرسش و داشتن جواب برای آن، به فرستنده پرسش، جواب را می‌فرستد. بدیهی است که برای این کار باید آدرس فرستنده هم درون پیام قرار گیرد، که در اینجا به ذکر جزئیات ساختار پیام نمی‌پردازیم.

فرستنده پس از دریافت جواب از بقیه عناصر، به روش میانگین وزن‌دار و از طریق فرمول زیر عمل استنتاج را انجام می‌دهد.

$$T_{final} = \frac{\sum_i T_i * Trust(e_s, e_i)}{\sum_i Trust(e_s, e_i)} \qquad (۱)$$

که در این فرمول، e_s فرستنده و e_i ها عناصری هستند که جواب می‌فرستند. مقدار T_i، مقدار اعتماد **مستقیمی** است که عنصر e_i به e_2 دارد و به e_s جواب می‌دهد و مقدار $Trust(e_s,e_i)$، مقدار اعتماد **مستقیمی** است که فرستنده پرسش به خود عنصر پاسخ‌دهنده دارد. اگر این مقدارِ $Trust(e_s,e_i)$ در هستان‌شناسی عنصر e_1 موجود نباشد، مقدار اعتماد اولیه که توسط مدیر اعتماد اختصاص داده شده در نظر گرفته می‌شود. روشن است که مقدار اعتماد بدست آمده از فرمول ۱ در همان محدوده مقادیر مجاز TrustValue قرار خواهد گرفت. در ضمن، بایستی برای دریافت پیام‌ها محدودیت زمانی قرار داد تا عمل استنتاج بیش از حد به طول نینجامد. حال موجودیت e_1 هستان‌شناسی خود را به روز می-کند. زمان استنتاج یعنی t نیز به عنوان یک صفت روی رابطه قرار می‌گیرد.

۴-۲- طریقه به روز رسانی مقادیر اعتماد

در مورد مقادیر اعتماد غیر مستقیم، نحوه به روز رسانی بدین شکل است که هر گاه هنگام ارزیابی قوانین به قانونی رسیدیم که محدودیت زمانی داشت، مثل قانونِ مثال ارائه شده در قبل، و هستان‌شناسی ما این محدودیت زمانی را ارضا نمی‌کرد، دوباره عملیات استنتاج را انجام می‌دهیم. یکی دیگر از راهکارهای موجود، تعیین یک دوره زمانی توسط مدیر اعتماد است که با اتمام آن دوره، دوباره عملیات استنتاج صورت پذیرد. علاوه بر این می‌توان این به روز رسانی را به خود هر

[13] Semantic Web Rule Language
[14] Broadcast

موجودیت واگذار نمود و محدودیتی روی آن اعمال نکرد. می‌توان ترکیبی از راهکار اول و دوم را نیز به کار گرفت.

برای به روز رسانی مقادیر اعتماد مستقیم، مکانیزم دیگری در مدل در نظر گرفته شده است. موجودیت‌ها پس از تعامل با یکدیگر می‌توانند نظر مستقیم خود را در مورد موجودیت طرف تعامل بیان کنند و در واقع پس از هر تعامل، مقدار اعتماد مستقیم به طرف دیگر تعامل، به روز می‌شود. این به روز رسانی از طریق فرمول ۲ انجام می‌شود:

$$T_{new} = \frac{T_{old} * collaborationNo + vote}{collaborationNo + 1} \qquad (۲)$$

که در آن، T_{old} مقدار اعتماد قبلی، collaborationNo تعداد تعاملات تا کنون با آن موجودیت و vote نظری است که از این تعامل جدید حاصل شده است. در واقع vote مقدار اعتمادی است که تنها از همین تعامل جدید و بدون توجه به سابقه قبلی بدست می‌آید. بدیهی است که مقدار vote باید در بازه مقادیر مجاز کلاس TrustValue باشد تا مقدار T_{new} نیز در همین بازه قرار بگیرد. در ضمن پس از این تعامل، صفت collaborationNo هم از طریق فرمول ۳ بدست می‌آید و در هستان‌شناسی به روز می‌شود.

$$collaborationNo = collaborationNo + 1 \qquad (۳)$$

سپس هر موجودیت مقدار اعتماد مستقیم جدید خود به موجودیت طرف تعامل را به مدیر اعتماد با یک پیام هشدار اعلام می‌کند. می‌توان این گسترش را نیز در مدل در نظر گرفت که این پیغام هشدار به سایر عناصر هم فرستاده شود و در آنها یک رویه به روز رسانی با توجه به این پیامهای هشدار تعریف گردد. البته این گسترش، هزینه‌های اضافی زیادی روی مدل به بار می‌آورد. چرا که پس از به روز رسانی هر عنصر، مقدار اعتماد جدید آن باید دوباره به بقیه فرستاده شود تا اینکه در نهایت سیستم به حالت پایداری برسد (مثلاً میانگین تغییر مقادیر از مقدار خاصی کمتر باشد).

۵- ارزیابی مدل

در این قسمت به ارزیابی مدل پیشنهادی مقاله می‌پردازیم. استنتاج از قوانین SWRL با الگوریتم Rete [15] انجام می‌گیرد. قالب تعریف قوانین به صورتی است که در طرف راست آنها، تنها اجازه تعامل داده می‌شود و یا داده نمی‌شود. به همین دلیل حداکثر جملاتی که استنتاج می‌شود، محدود بوده و تابعی از تعداد عناصر فراگیر و تعداد رسته‌های اعتماد خواهد بود. بنابراین با توجه به اینکه در قوانین دور وجود ندارد، مدل تصمیم‌پذیر و زمان پاسخ‌دهی آن با توجه به تعداد محدود عناصر و رسته‌ها در هر دامنه قابل قبول می‌باشد.

مدل پیشنهادی دارای الگوریتم‌های ساده‌ای برای استنتاج اعتماد و به روز رسانی مقادیر اعتماد است و این سادگی برای محیط‌های فراگیر که ابزارهای آن دارای محدودیت‌هایی از نظر اندازه و عمر باتری می‌باشند، اهمیت زیادی دارد.

یکی از ویژگیهای عناصر فراگیر، خودمختاری آنهاست که در مدل به طور کامل در نظر گرفته شده است. برای هر عنصر ساختار کلی هستان‌شناسی یکتاست ولی هر یک می‌توانند خط‌مشی‌های خود را برای تصمیم‌گیری داشته باشند که در این مقاله مثال‌هایی از آن را نشان دادیم اگر چه به ذکر جزئیات تعریف این قوانین نپرداختیم.

شاید، مهمترین ویژگی مدل پیشنهادی که آن را از بقیه متمایز می‌کند، در نظر گرفتن ارتباط معنایی میان رسته‌های اعتماد می‌باشد که در بخش‌های قبل، توضیح داده شد. به عنوان نمونه، اگر اعتماد به منبعی در زمینه ارائه سرویس اینترنت زیاد باشد، در زمینه ارائه سرویس ایمیل نیز می‌توان به این منبع اعتماد زیادی داشت. بنابراین می‌توان قوانینی تعریف نمود که این روابط معنایی را نیز بپوشانند و این انعطاف-پذیری در تعریف خط‌مشی‌های امنیتی یکی از خصوصیات منحصر به فرد این مدل می‌باشد.

با استفاده از ساختار هستان‌شناسی در مدل، امکان گسترش مدل و تعریف روابط جدید نیز امکان‌پذیر می‌باشد. با توجه به این امر، یکی از مزایای مدل امکان افزودن متغیرهای زمینه به آن است. می‌توان به سادگی یک سلسله مراتب از متغیرهای زمینه را به ساختار هستان‌شناسی افزود و روابط دلخواه مطرح در آن محیط فراگیر را نیز به این ساختار اضافه کرد. به عنوان نمونه می‌توان با تعریف رابطه‌ی hasLocation در هستان-شناسی، متغیر زمینه مکان یک عنصر را به هستان‌شناسی افزود. همانطور که می‌دانیم زمینه یکی از پارامترهای مهم

محیط‌های فراگیر است و با اضافه کردن این مفهوم به مدل می‌توان قوانینی تعریف نمود که تا حد زیادی مفهوم زمینه را نیز بپوشانند.

۶- نتیجه‌گیری و کارهای آینده

در این مقاله مدلی بر مبنای ساختار هستان‌شناسی برای استنتاج اعتماد در محیط‌های فراگیر ارائه کردیم که علاوه بر در نظر گرفتن مسأله اعتماد، مقادیر صریح اعتماد را نیز به عناصر مختلف اختصاص می‌دهد.

برای بیان هستان‌شناسی از زبان رایج OWL و برای بیان قوانین و استنتاج از آنها، از SWRL استفاده می‌شود. ضمناً سادگی رویه استنتاج موجود در مدل به ما امکان می‌دهد که بدون صرف هزینه زیاد، این روش را در محیط‌های فراگیر اعمال کنیم. همانطور که می‌دانیم در محیط‌های فراگیر، محدودیت‌هایی مانند کوچکی و عمر کم باتری‌ها وجود دارد که باید در نظر گرفته شوند.

در نظر گرفتن روابط معنایی میان رسته‌های اعتماد از دیگر مسائلی بود که در مدل‌های قبل، به آن توجهی نشده بود و ما در اینجا علاوه بر سلسله مراتب میان عناصر فراگیر، این مسأله را نیز لحاظ کردیم و امکان تعریف قوانین امنیتی با انعطاف-پذیری بسیار بالاتری را ایجاد نمودیم.

در ادامه کار در نظر داریم تا با افزودن مفهوم زمینه و تعریف ساختار دقیق پیام‌های پروتکل ارتباطی، به سمت پیاده‌سازی این مدل حرکت کنیم. یکی دیگر از مزایای این مدل سادگی آن در بحث پیاده‌سازی است که می‌توان با زبانهای شناخته شده‌ی وب‌معنایی، هستان‌شناسیِ اعتماد را توصیف نمود.

۷- مراجع

[1] L. Kagal, T. Finin, and A. Joshi. "*Moving from Security to Distributed Trust in Ubiquitous Computing Environments*", IEEE Computer, December 2001.

[2] M. Blaze, J. Feigenbaum, and A. D. Keromytis. "*The role of trust management in distributed systems security*", Proceedings of the Secure Internet Programming, pages 185-210, 1999.

[3] C. English, P. Nixon, S. Terzis, A. McGettrick and H. Lowe. "*Dynamic Trust Models for Ubiquitous Computing Environments*", Proceedings of the Ubicomp Security Workshop, 2002.

[4] M. Satyanarayanan. "*Pervasive computing: Vision and Challenges*", IEEE Personal Communications , Vol. 8, No. 4, pages 10-17, Aug 2001.

[5] G. A. Golbeck. "*Computing and applying trust in web-based social networks*," Ph.D. dissertation, University of Maryland, 2005.

[6] A. Josang, R. Hayward, and S. Pope. "*Trust network analysis with subjective logic*," Proceedings of the Australasian Computer Science Conference *(ACSC2006)*, 2006.

[7] N. Griffiths, K.-M. Chao, and M. Younas. "*Fuzzy Trust for Peer-to-Peer systems*", Proceedings of the P2P Data and Knowledge Sharing Workshop (P2P/DAKS 2006), at the 26th International Conference on Distributed Computing Systems (ICDCS 2006), Lisbon, Portugal, July 2006.

[8] H. Chen, F. Perich, T. Finin, and A. Joshi. "*SOUPA: Standard Ontology for Ubiquitous and Pervasive Applications*", Proceedings of the 1st Annual International Conference on Mobile and Ubiquitous Systems (MobiQuitous 2004) and Networking and Services, IEEE Computer Society, pages 258-268, Cambridge, MA, USA, August 2004.

[9] H. Chen, T. Finin, and A. Joshi. "*A Pervasive Computing Ontology for User Privacy Protection in the Context Broker Architecture*", Computer Science and Electrical Engineering, University of Maryland, July 2004.

[10] A. Abdul-Rahman and S. Hailes. "*A Distributed Trust Model*", Proceedings of the New Security Paradigms Workshop, ACM Press, pages 48–60, 1998.

[11] F.Almenarez, A.Marin, C. Campo, and C. Garcia. "*PTM: A Pervasive Trust Management Model for Dynamic Open Environments*", Proceedings of the First Workshop on Pervasive Security, Privacy and Trust PSPT'04, 2004.

[12] F.Almenarez, A.Marin, D. Diaz, and J. Sanchez. "*Developing a Model for Trust Management in Pervasive Devices*", Proceeding of the Fourth Annual IEEE International Conference on Pervasive Computing and Communications Workshop (PERCOMW'06), 2006.

[13] Ubiquitous Networks with a Secure Provision of Services, Access, and Content Delivery. http://www.it.uc3m.es/pervasive

[14] L. Kagal, T. Finin, and A. Joshi. "*Trust-based security in pervasive computing environments*", IEEE Computer, Vol. 34 No. 12, pages 154-157, December 2001.

[15] C. Forgy. "Rete: A Fast Algorithm for the Many Pattern/ Many Object Pattern Match Problem", Artificial Intelligence 19, pages 17-37, 1982.