کنترل دسترسی آگاه از زمینه و مبتنی بر تاریخچه در محیط های محاسباتی فراگیر

آزاده عمرانی*، ساره سادات امامی‡، مرتضی امینی◊

دانشگاه صنعتی امیرکبیر- دانشکده کامپیوتر omrani@ce.aut.ac.ir *

دانشگاه خواجه نصیرالدین طوسی- دانشکده برق emami@ee.kntu.ac.ir ‡

دانشگاه صنعتی شریف- دانشکده کامپیوتر morteza_amini@mehr.sharif.ir ◊

چکیده - ظهور ابزارهای هوشمند، وسایل سیار و حسگر ها، امکانات لازم را برای ایجاد محیط های محاسباتی فراگیر فراهم کرده است. در این محیط ها تقابل کاربران با اطلاعات به صورت هر جا و هر زمان انجام می شود. این محیط ها چالش های امنیتی خاص خود را دارند. یکی از مهمترین این چالش ها کنترل دسترسی به اطلاعات فراگیر است. اطلاعات زمینه ای می تواند از جمله عوامل مهم دخیل در کنترل دسترسی در این محیط ها باشد. از طرف دیگر دسته ای از مکانیزمهای کنترل دسترسی وجود دارند که بر اساس تاریخچهٔ دسترسی ها کار می کنند به این ترتیب که سیستم، تاریخچه ای از دسترسی هایی که یک کاربر یا پروسس تا کنون انجام داده است را نگهداری می‌کند و از این اطلاعات برای تصمیم گیری استفاده می‌کند. در این پژوهش مدلی ارائه می شود که از هر دو عامل اطلاعات زمینه ای و اطلاعات تاریخچه ای برای کنترل دسترسی در محیط های محاسباتی فراگیر استفاده می‌کند. این مدل بر اساس مدل کنترل دسترسی نقش مبنا عمل می‌کند.

کلید واژه - کنترل دسترسی آگاه از زمینه، کنترل دسترسی مبتنی بر تاریخچه، گراف محدودیت، مدل کنترل دسترسی نقش مبنا

1- مقدمه

در آینده نزدیک محاسبات فراگیر و فناوری ارتباطات وارد زندگی روزمرهٔ افراد شده و به تدریج شیوهٔ تقابل اطلاعات، تقابل انسانها با یکدیگر و با دنیای اطراف خود را دگرگون می‌کند. ظهور ابزارهای هوشمند، وسایل سیار، PDAها و حسگر ها، امکانات لازم را برای ایجاد محیط های محاسباتی فراگیر[1] فراهم کرده است که در نتیجهٔ آن فضاهای فیزیکی معمولی به فضاهای هوشمند بدل می‌شوند. در چنین فضاهایی، یک ساختار دسترسیِ هر جا و هر زمان به اطلاعات بوجود می آید. یکی از چالش های اساسی در این محیط ها مدیریت امنیت و کنترل دسترسی است. اولین چیزی که برای کنترل دسترسی به ذهن می رسد استفاده از لیست کنترل دسترسی است که در آن لیست کاربران مجاز برای دسترسی به یک شیء خاص ذکر شده است. اما در محیطهای محاسباتی فراگیر اختیارات دسترسی کاربر تنها به هویت کاربر بستگی ندارد. بلکه چگونگی وضعیت کاربر و وضعیت سیستم در حال حاضر و سابقه دسترسی های وی نیز می تواند روی اختیارات کاربر تأثیر داشته باشد. به چگونگی وضعیت کاربر و وضعیت سیستم، اطلاعات زمینه ای یا به اختصار زمینه[2] گفته می شود. از طرف دیگر تاریخچه دسترسی‌ها به تنهایی از اهمیت بالایی

[1] Pervasive Computing Environment

2 context

برخوردار است زیرا بسیاری از محدودیت‌ها بدلیل دسترسی-های قبلی یک کاربر می تواند به وجود بیاید و ریشه‌ای در اصل و طبیعت کاربر ندارد. بیشتر مدل‌هایی که تاکنون در کنترل دسترسی محیط‌های فراگیر حساس به زمینه ارائه شده بر مبنای مدل RBAC [5] طراحی گردیده است. گرچه در آنها از مدلی استفاده شده که از کامل‌ترین مدل-های کنترل دسترسی می‌باشد و بسیاری از نیازها را برطرف می‌کند اما اشاره‌ای به تاریخچه و اثر آن بر کنترل دسترسی نشده است. ما بر آنیم تا مدلی برای کنترل دسترسی حساس بر زمینه[3] و مبتنی بر تاریخچه[4] بر مبنای مدل RBAC در محیطهای محاسباتی فراگیر ارائه دهیم. ما در این مدل تاریخچه را در کنار زمینه‌های موجود در نظر می گیریم. سیستم ما در طرف کاربر یک ماشین حالت از نقشهای مجاز وی تشکیل می دهد. ضمنا این سیستم دارای یک ماتریس برای نگه داری تاریخچه اعمالی است که نقش ها روی شیء های مختلف انجام داده اند و بر اساس این اطلاعات و گراف محدودیت یا ماشین حالت تغییر انتساب کاربر به همراه اطلاعات زمینه ای برای تعیین نقش فاعل ها و تعیین اجازه دسترسی به اشیاء و در نتیجه کنترل دسترسی های آینده این فاعل ها تصمیم گیری می‌کند.

ساختار ادامه این مقاله به این ترتیب است که در بخش2 کار های مرتبط بررسی می شود، در بخش 3 کنترل دسترسی مبتنی بر زمینه را توضیح می دهیم، در بخش4 نقش تاریخچه را تبیین می کنیم، سپس در بخش 5 یک مدل حساس بر زمینه و مبتنی بر تاریخچه بر اساس مدل نقش مبنا ارائه می شود و در نهایت در بخش 6 نتیجه گیری خواهیم کرد.

2- کارهای انجام شده

در کاری که Zhang و همکارانش انجام داده اند یک مکانیزم کنترل دسترسی پویای آگاه از زمینه(DRBAC[5]) ارائه شده که با توجه به زمینهٔ مربوطه به صورت پویا به کاربران اختیاراتشان را تفویض می‌کند. در این مکانیزم به نوعی مدل RBAC را توسعه داده اند بطوریکه مزایای این مدل (توانایی تعریف و مدیریت خط مشی های امنیتی پیچیده) حفظ شود. در این مدل برای داشتن زمینه هر کاربر همراه با آن یک عامل وجود دارد که زمینه آن را بر اساس معیارهای مورد نظر بدست می‌آورد. [1]

در کار Hengartner و همکارش کنترل دسترسی بطور کلی در محیطهای محاسباتی فراگیر مورد بررسی قرار گرفته است. در این مقاله سه اصل برای طراحی معماری یک مکانیزم کنترل دسترسی در محیط محاسباتی فراگیر پیشنهاد شده است تا براین مشکلات غلبه کند. در طراحی این اصول سعی شده که از اطلاعات زمینه ای برای کنترل دسترسی استفاده شود.[2]

در کار Edjlali و همکارانش از مکانیزیمی بر مبنای تاریخچه برای مقابله با حلمهٔ ممانعت از سرویس استفاده شده است. در این مقاله مناطق قابل دسترسی توسط کد سیارتوسط خط مشی کنترل دسترسی OOok[6] بصورت پویا تعیین می شوند، به این صورت که برنامه ها بر حسب رفتار قبلی خود به کلاسهای معادلی طبقه بندی می شوند و یک برنامه با توجه به اعمالی که انجام می دهد در یکی از این سه دسته قرار می گیرد و از آن به بعد این برنامه فقط به منابع قابل دسترس توسط این دسته دسترسی دارد. [3]

Brewer و همکارانش خط مشی امنیتی دیوار چینی[7] را که یک خط مشی امنیتی مبتنی بر تاریخچه است ارائه کرده‌اند. این خط مشی یک خط مشی اقتصادی مهم است که در حوزهٔ علوم کامپیوتر بکار می‌رود. در این مدل، دسترسی به داده توسط خصوصیات داده محدود نمی‌شود بلکه توسط داده‌هایی محدود می‌شود که یک فاعل قبلاً به آنها دسترسی داشته‌است. خط مشی دیوار چینی دارای جنبه های پویا هم هست.[4]

3 Context-Aware
4 History-Based
5 Dynamic Role Based Access Control
6 One-out-of-k
7 Chinese wall security policy

3- کنترل دسترسی مبتنی بر زمینه

در محیط های محاسباتی فراگیر که اکثر کاربران سیار هستند و با وسایل بی سیم سیار به سرویس ها، اطلاعات و حسگرها دسترسی پیدا می کنند، اطلاعات زمینه ای کاربر شامل مکان کاربر، زمان، منابع سیستم، وضعیت شبکه و پیکرندی امنیتی سیستم و غیره است. این اطلاعاتِ زمینه ای در محیط بصورت کاملاً پویا تغییر می‌کند و تغییر آن می تواند روی دسترسی ها و اختیارات کار بران تأ ثیر بگذارد. به این ترتیب حتی ممکن است یک کار بر مجاز به سیستم آسیب برساند چون ممکن است در زمینه های مختلف نیازمندی های امنیتی سیستم متفاوت باشد. با استفاده از اطلاعات زمینه‌ای و اثر دادن آنها در کنترل دسترسی از استفاده نادرست از اطلاعات جلوگیری می‌شود. بنا براین نیاز به یک مکانیزم کنترل دسترسی دقیق تر که اختیارات کاربرها را بصورت پویا و با توجه به اطلاعات زمینه ای تعیین کند، احساس می شود.

بحث آگاهی از زمینه و بدست آوردن زمینه و بهنگام سازی اطلاعات زمینه‌ای خود از مسائل مهم می‌باشد. برای مثال بدست آوردن اطلاعات مکانی کاربر می تواند از طریق سیستم GPS باشد. نحوه ارسال اطلاعات زمینه‌ای نیز باید از امنیت برخوردار باشد تا قابل جعل از طریق کاربران نباشد. ضمناً بهنگام سازی باید در اطلاعات زمینه‌ای کاربر نیز انجام شود به طوری که در زمانی که کاربر در حال دسترسی به بخشی از شبکه است چنانچه اطلاعات زمینه‌ای وی (مثلا مکان او) تغییر کرد در نوع دسترسی او اثر بگذارد.

4- کنترل دسترسی مبتنی بر تاریخچه

یک نمونه از یک خط مشی مبتنی بر تاریخچه در سرورهای log-in دیده می شود. در این سرورها به هر کاربر یک نام کاربری و کلمهٔ عبور داده می شود تا به سرویسهای مربوطه دسترسی پیدا کنند. برای جلوگیری از حملهٔ brute-force برای کشف کلمه های عبور، این خط مشی پیاده می شود که: "پس از این که یک کاربر بیش از سه بار موفق به ورود به سیستم نشد، برای تلاش بار چهارم باید 30 ثانیه صبر کند." در این حالت باید تاریخچهٔ تعداد تلاش های ناموفق در سیستم حفظ شود.

علاوه بر این، خط مشی دیگری بنا به ماهیت عملیاتی سیستم(مثلا یک شرکت اقتصادی) بر مبنای تاریخچه دسترسی‌های هر کاربر می تواند پیاده شود به این صورت که اگر کاربری بخواهد در نقش مشاور مالی به شرکتی خدمات ارائه کند، در صورتیکه قبلا به اطلاعات مالی شرکت رقیب دسترسی پیدا کرده باشد، قادر نخواهد بود به اطلاعات مالی این شرکت دسترسی پیدا کند. این تغییر امکانات دسترسی در عین حال می تواند با تغییر زمینه کاربر نیز اتفاق بیفتد.

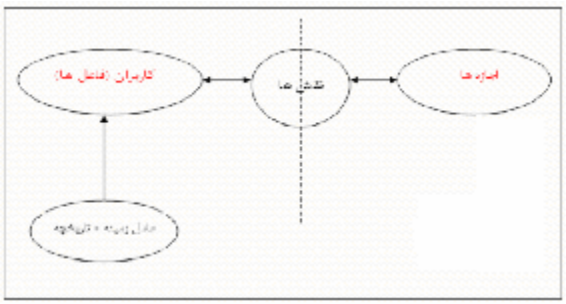
5- مدل کنترل دسترسی حساس بر زمینه و مبتنی بر تاریخچه بر اساس مدل نقش مبنا

با توجه به استفاده از مدل کنترل دسترسی نقش مبنا عناصر زیر در این سیستم وجود دارند: *کاربران* که قرار است دسترسی های آنان کنترل شود. این کاربران لزوما کاربران انسانی نیستند بلکه ممکن است برنامه هایی باشند که توسط رخداد یک تغییر در زمینه فعال شده و درخواست دسترسی به منبعی را داشته باشند. *نقش* که یک کارکرد متناسب با یک مسؤولیت و اختیار خاص در سازمان است. *اجازه‌ها* که انواع دسترسی‌ها به اشیاء و منابع سیستم هستند. *جلسه* که مجموعه‌ای از تعاملات بین فاعل‌ها (کاربرها) و اشیاء به طوریکه به هر کاربر در طول هر جلسه مجموعه‌ای از نقش ها نسبت داده می شود که در هر زمان ممکن است همه آن نقش‌ها فعال نباشند. *انتساب کاربر* که نگاشت نقش‌ها به کاربران را تعیین می‌کند. نقش فعال از میان نقشهای منتسب به کاربر، توسط عامل هایی تعیین می‌شود. *انتساب اجازه* که نگاشت اجازه‌ها به نقش‌ها را تعیین می‌کند.

هنگامی که کاربری به سیستم وارد می‌شود و یک جلسه باز می‌کند، متولی مرکزی سیستم[8] برحسب توانایی های کاربر نقش‌های اولیه ممکن برای وی را در این جلسه به وی منتسب می‌کند. این نقش‌ها در واقع یک زیر سلسله مراتب از سلسله مراتب نقش‌های کل سیستم هستند. سپس متولی

8 Central Authority

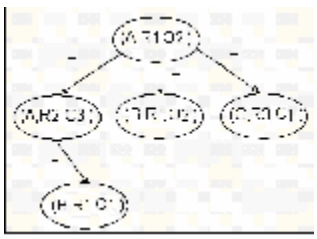
مرکزی یک عامل را برای جمع آوری مقادیر متغییرهای زمینه‌ای و تاریخچه دسترسی‌های وی برای کنترل دسترسی‌های کاربر راه اندازی می‌کند. این عامل نقش فعال کاربر در جلسه را نیز تعیین می‌کند. شمای کلی این مدل در شکل 1 نشان داده شده است.



شکل1 – مدل کنترل دسترسی

برای در نظر گرفتن اطلاعات زمینه‌ای و تاریخچه‌ای در کنترل دسترسی، اجزای زیر نیز در سیستم تعریف می‌شوند:

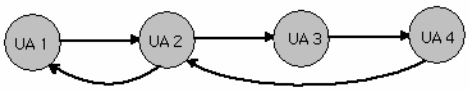
متغییر های زمینه: تعدادی متغییر که مقادیر آنها وضعیت محیط را نشان می‌دهد. *متغییر های رخداد دسترسی:* متغییر هایی هستند که در آنها وقوع دسترسی نقشها با اجازه هایشان روی اشیای سیستم ثبت می‌شود. *عامل کنترل دسترسی:* عاملی است که در آغاز ایجاد یک جلسه در طرف کاربر تشکیل می‌شود. یک مسؤولیت این عامل جمع آوری اطلاعات زمینه ای مربوط به کاربر مورد نظر و تعیین مقادیر متغییر های زمینه است. علاوه بر این، عامل مورد نظر بر جلسات نیز نظارت دارد به طوریکه می‌تواند تراکنش های کاربران در قالب نقش ها با اشیاء را مشاهده کرده و در متغییرهای رخداد دسترسی نگهداری کند. *ماتریس رخداد دسترسی:* ماتریسی است سه بعدی که ابعاد آن را نقش‌ها، اجازه‌ها و اشیاء تشکیل می‌دهند. هر عنصر این ماتریس یک مقدار دو حالته است. در صورتیکه نقشی عملا از اجازه ای روی شیئ‌ای استفاده کند مقدار عنصر متناظر با آن نقش و آن اجازه و آن شیئ در ماتریس، مقدارTrue و در غیر این صورت مقدار False به خود می-گیرد. مقدار اولیه تمام عناصر این ماتریس False است. این ماتریس در متولی مرکزی سیستم نگهداری شده و در اختیار عامل‌های کنترل دسترسی قرار می‌گیرند. *ماشین حالت نقش ها:* عامل کنترل دسترسی هر کاربر در طرف کاربر یک ماشین حالت ایجاد می‌کند که هر حالت از آن یک نقش از زیرسلسله مراتب نقشهای ممکن آن کاربر در سیستم است. تغییر اطلاعات زمینه‌ای می‌تواند حالت این ماشین را عوض کند و به عبارت دیگر نقش فعال کاربر را تعیین کند. در مثالی که در پیوست این مقاله آورده شده یک نمونه از تبدیل زیرسلسله مراتب نقش‌ها به ماشین حالت نقش‌ها دیده می‌شود. *گراف محدودیت:* می‌توانیم برای به کارگیری تاریخچه از یک گراف برای محدودیت دسترسی‌ها استفاده کنیم. این گراف بر اساس قوانین حاکم بر سیستم از طرف مدیر سیستم تهیه شده و در متولی مرکزی سیستم نگه داری می‌شود و تایید هر مجوز از طریق آن بررسی می‌گردد. رأس های این گراف تشکیل شده از یک سه تایی مرتب است که شامل زیر مجموعه ای از دسترسی ها، یک نقش و یک شیئ است و بر چسب یالها یک متغیر منطقی است. فرض کنید یالی از رأس (A , R2, O3) به رأس (B , R1, O1) وجود دارد، اگر این یال دارای برچسب True باشد به این معنی است که یک کاربر با نقش R1 در صورتی می‌تواند دسترسی های B را روی شیئ O1 داشته باشد که قبلا با نقش R2 دسترسی های A را روی شیئ O3 داشته است و اگر این برچسب مقدار False را داشت نیز به معنی این است که کاربری با نقش R1 نمی‌تواند دسترسی های B را روی شیئ O1داشته باشد اگر در گذشته با نقش R2 دسترسی A را روی شیئ O3 داشته است. در شکل 2 نمونه ای از این گراف را می‌بینید. لازم به ذکر است که این گراف یک گراف جهت دار بدون سیکل است که حداقل یکی از رأسهای آن به عنوان ریشه معرفی می‌شوند.



شکل2-گراف محدودیت

ماشین حالت تغییر انتساب کاربر: در مواردی که تشکیل گراف محدودیت به دلیل پیچیده شدن یا زیاد شدن تعداد رأس های گراف ممکن نباشد از ماشین حالت تغییر انتساب کاربر برای به کارگیری تاریخچه در محدودیت دسترسی ها استفاده می‌کنیم. این ماشین حالت توسط عامل کنترل دسترسی هر کاربر در طرف کاربر نگهداری می‌شود. هر

حالت در این ماشین حالت شامل مجموعه ای از نقش هاست که در آن حالت برای کاربر مورد نظر مجاز تلقی می-شود و در واقع یک انتساب کاربر است. تغییر متغییرهای رخداد دسترسی که توسط عامل کنترل دسترسی احساس می‌شود باعث تغییر حالت در این ماشین می‌شود. این ماشین حالت برای یک کاربر خاص در شکل 3 نشان داده شده است.



شکل3- ماشین حالت تغییر انتساب کاربر

در آغاز یک جلسه کاربر، عامل کنترل دسترسی کاربر فعال شده و زیر سلسله مراتب مربوط به این کاربر را از متولی مرکزی سیستم دریافت می‌کند. سپس ماشین حالت نقش ها را به تناظر آن می‌سازد که در آن یکی از حالتها، نقش فعال کنونی را نشان می‌دهد. بنا به تعریف محیط، ممکن است عامل کنترل دسترسی، نسخه ای از گراف محدودیت را نیز همزمان از متولی مرکزی سیستم دریافت کند یا اینکه ماشین حالت تغییر انتساب کاربر با مشخص بودن حالت جاری را بارگذاری کند.

ابتدا حالتی را در نظر می‌گیریم که که از گراف محدودیت استفاده شود. در این حالت نقش فعال کاربر توسط ماشین حالت نقش ها (با توجه به تغییر زمینه وی) مشخص می-شود. کاربر در این نقش درخواست اجازه دسترسی خاصی را به عامل کنترل دسترسی خود می‌دهد. عامل کنترل دسترسی سه‌تایی اجازه-نقش-شیئ را در گراف محدودیت پیدا می‌کند. در صورتیکه سه‌تایی مورد نظر در گراف یافت نشد یعنی در این دسترسی تاریخچه اهمیتی ندارد و با توجه به سایر معیار ها داده می‌شود. اگر رأس مورد نظر یافت شد، آنگاه در گراف محدودیت به سمت عقب حرکت کرده و شرایط هر گره از این گراف را در ماتریس رخداد دسترسی بررسی می‌کند. در نهایت اگر در این مسیر تا ریشه درخت، عنصر متناظر با سه‌تایی‌های اجازه-نقش-شیئ در ماتریس رخداد دسترسی با برچسب یالهای رو به پایین آنها تطابق داشت دسترسی اعطا می‌شود.

در حالتی که از ماشین حالت تغییر انتساب کاربر استفاده شود نیز نقش فعال کاربر توسط ماشین حالت نقش ها مشخص می شود. در این حالت نیازی به نگهداری ماتریس رخداد دسترسی وجو ندارد. حالت جاری در ماشین حالت تغییر انتساب کاربر نیز مشخص است. باید دقت کنیم که برای حفظ سازگاری، مجموعه نقش های یک کاربر در یک حالت از ماشین حالت تغییر انتساب کاربر باید برابر با کلیه نقش های ماشین حالت نقش‌ها در آن لحظه باشد. کاربر در این نقش درخواست اجازه دسترسی خاصی را به عامل کنترل دسترسی خود می دهد. عامل کنترل دسترسی با توجه به نقش کاربر و انتساب اجازه ها به آن نقش، دسترسی لازم را اعطا می‌کند. در صورتیکه این اعطا یا عدم اعطای اجازه که به تغییر متغییر های رخداد دسترسی می-انجامد باعث تغییر حالت در ماشین حالت تغییر انتساب کاربر بشود، یعنی وقوع یا عدم وقوع یک دسترسی در یک نقش به صورت پویا مانع از وقوع دسترسی های مجاز دیگر(تصدی نقش های دیگر) برای این کاربر در آینده شود، آنگاه عامل کنترل دسترسی به تناسب این رخداد حالت جاری در ماشین حالت تغییر انتساب کاربر را عوض کرده و نقشهایی از کاربر را که از این پس غیر مجاز شناخته خواهند شد از سلسله مراتب نقشهای کاربر (از ماشین حالت نقش های وی) حذف می‌کند و به این ترتیب دیوار بازدارنده مورد نظر را ایجاد می‌کند. این تغییرات به اطلاع متولی مرکزی سیستم می‌رسند تا برای آغاز جلسات بعدی زیرسلسله مراتب به روز شده را در اختیار عامل ها قرار دهد. در اینجا می‌توان موضوع تاریخچه را گسترده تر از وقوع یک دسترسی در گذشته در نظر گرفت و مثلا تعداد دسترسی-های غیر مجاز(متناسب با زمینه) یا عملیات گذشته هر نقش را نیز به تناسب نیازهای سازمان در نظر گرفت.

برای تبیین عملکرد سیستم در این حالت با استفاده از یک مثال به پیوست مراجعه شود.

6- نتیجه گیری

در این مقاله موضوع کنترل دسترسی به اطلاعات فراگیر مورد بررسی قرار گرفت و مدلی ارائه شد که از هر دو عامل اطلاعات زمینه ای و اطلاعات تاریخچه ای برای کنترل دسترسی در محیط های محاسباتی فراگیر استفاده می‌کند. این مدل بر اساس مدل کنترل دسترسی نقش مبنا عمل می‌کند و برای اعمال اثر تاریخچه در آن دو روش پیشنهاد

شد. بر اساس تاریخچه محدودیت های جدیدی را می توان روی سیستم اعمال کرد که پویایی بیشتری به سیستم کنترل دسترسی می‌دهد طوریکه بر اساس اطلاعات زمینه-ای موجود به تنهایی نمی‌توان این پویایی را در تصمیم‌گیری اعمال کرد. این امر پویایی سیستم در محیط های محاسبات فراگیر را افزایش می‌دهد.

مراجع

[1] Zhang, G. and Parashar, M. "Context-Aware Dynamic Access Control for Pervasive Applications". In Proceedings of the Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2004), 2004 Western MultiConference (WMC), January 2004.

[2] Urs Hengartner and Peter Steenkiste, "Access Control to Information in Pervasive Computing Environments", Ninth Workshop on Hot Topics in Operating Systems (HotOS IX), ACM, May 2003, pages 157-162.

[3] Guy Edjlali , Anurag Acharya , Vipin Chaudhary, "History-based access control for mobile code", Proceedings of the 5th ACM conference on Computer and communications security, p.38-48, November 02-05, 1998.

[4] Brewer، D.F.C and Nash، M.J. "The Chinese Wall Security Policy." IEEE Symposium on Security and Privacy، 215-228 ,1989.

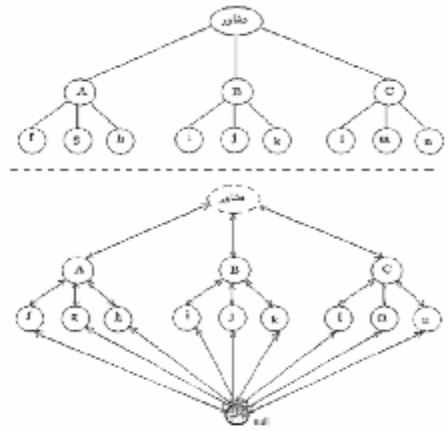
[5] S. Gavrila D. R. Kuhn D. F. Ferraiolo, R. Sandhu and R. Chandramouli. "Proposed nist standard for role based access control". ACM Transactions on Information and System Security, 4(3):224–274, 2001.

7- پیوست : یک مثال از مدل

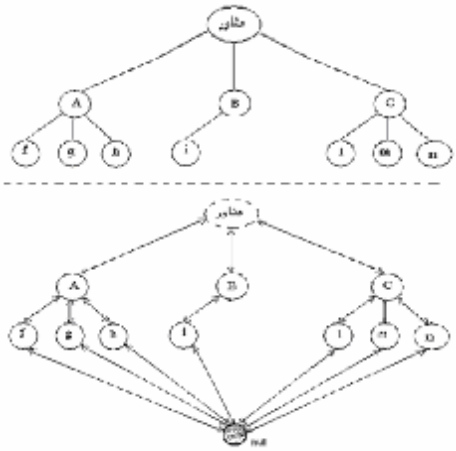
محیط یک شرکت مشاوره مالی و سرمایه گذاری(بنگاه) را در نظر می گیریم. این بنگاه یک قسمت مخصوص خدمات مشاوره ای و ارتباط با مشتریان بنگاه دارد. دسته ای از مشتریان این بنگاه، شرکتهایی هستند که می توانند به بنگاه سفارش خرید و فروش سهام برای خود بدهند، اطلاعات مربوط به پرتفولیو (سبد) سهام خود، در خصوص سهامی که توسط این شرکت خریداری شده را به دست بیاورند و یا در مورد سرمایه گذاری درانواع اوراق بهادار خدمات مشاوره ای دریافت کنند. این بنگاه می تواند مدیریت منابع مالی مشتریان خود را نیز به عهده بگیرد. توضیحاً اضافه می شود مسؤولیت اجتماعی بنگاه عبارت از «تلفیق عملیات و ارزش های بنگاه به گونه ای که منافع همه ذینفعان از جمله مشتریان، کارکنان وسهامداران در سیاست ها و رفتار بنگاه ملحوظ گردد».

محیط این بنگاه یک محیط محاسباتی فراگیر است. لذا اطلاعات ساختمان، افراد و فعالیت های آنان در بنگاه با توجه به میزان حساسیت آن باید درهر زمان در دسترس باشد و محیط نسبت به آنها عکس العمل نشان می دهد. با توجه به مسؤولیت اجتماعی بنگاه و برخی ملاحظات دیگر (مثل حفظ حریم خصوصی)، علیرغم وجود محیط محاسباتی فراگیر در این بنگاه، داده ها و اطلاعاتی وجود دارندکه باید از دید برخی بخش های بنگاه مخفی بمانند. این بنگاه مثلاً از سه بخش مشاوره ای کلی تشکیل شده است: ارائه خدمات به شرکتهای نفتی، ارائه خدمات به شرکتهای کشاورزی و ارائه خدمات به شرکتهای بانکی. می بینیم که این سه بخش متناظر با کلاس های تضاد منافع در مدل دیوار چینی هستند. لذا نقشهایی که در گیر ارائه خدمات به شرکت نفتی A هستند اجازه ندارند به شرکت نفتی B خدمات مشاوره ای ارائه کنند چون این نقشها از ریز گردش های مالی و سرمایه گذاری های آینده شرکت نفتی A مطلع اند و شرکت نفتی B نیز رقیب شرکت نفتی A محسوب می شود. در این محیط کارمند A در ساعت اداری وارد بنگاه می شود. هویت وی از طریق یک مکانیزم امنیتی تصدیق اصالت محرز شده و با توجه به نقشی که برای وی تعریف شده (مشاور) فقط به سرویس های طبقه مشاوره بنگاه دسترسی خواهد داشت. به محض ورود کارمند A به سیستم از طرف متولی مرکزی سیستم سلسله مراتب نقشهای تعریف شده برای وی (شکل4) به عامل کنترل دسترسی این کاربر(روی کامپیوتر بی سیم وی) معرفی می شود. ماشین حالت نقش در عامل کنترل دسترسی تشکیل می شود. هم اکنون نقش کلی مشاور برای این کاربر فعال است (نقش نقطه چین) و می تواند به سرویس های عمومی این نقش در طبقه مشاوره بنگاه دسترسی داشته باشد. فرض می کنیم این کارمند به تازگی

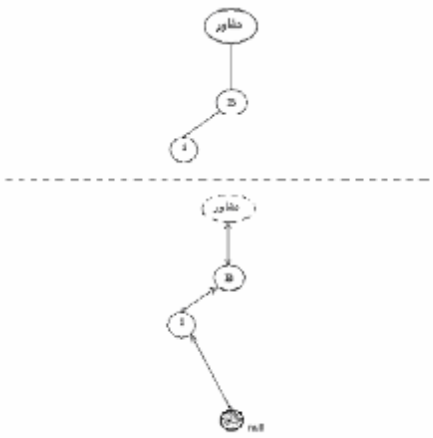
کار روی یک پرونده را به اتمام رسانده و امروز باید پرونده جدیدی برای کار انتخاب کند. او وارد بخش مشاوره شرکت های کشاورزی می شود. به محض ورود وی به این بخش (تغییر زمینه حضور وی)نقش فعال وی به نقش مشاور شرکت های کشاورزی(B در شکل4) تغییر می‌کند. وی در این نقش تعداد دسترسی های تخصصی بیشتری دارد اما فقط روی اطلاعات عمومی شرکتهای مشتری در بخش کشاورزی. در این حالت کارمند A می تواند جابجا شده و برای انتخاب کار تازه خود در نقش مشاور شرکت های نفتی(C در شکل4) جوانب کار آتی خود را بررسی کند. در این موارد تغییر مکان کاربر به عنوان یک اطلاعات زمینه ای باعث تغییر حالت در ماشین حالت نقش ها در کاربر می شود بدون اینکه خود ماشین حالت تغییر کند. اما اکنون کارمندA تصمیم دارد به شرکت i در بخش کشاورزی مشاوره بدهد. به محض اینکه اولین دسترسی وی به اطلاعات حساس شرکت i رخ داد، عامل کنترل دسترسی، ماشین حالت نقشها را به صورت شکل 5 در می آورد و این تغییر را برای متولی مرکزی نیز می فرستد. متولی مرکزی وظیفه دارد از این پس(در جلسات آتی) برای کارمند A سلسله مراتب شکل 5 را معرفی کند. به این ترتیب قانون Simple-Secutity در مدل دیوار چینی برقرار می شود. از طرف دیگر با توجه به خاصیتProperty-* در مدل دیوار چینی علاوه بر قانون فوق برای نوشتن روی یک سند حساس نباید هیچ سند دیگری که در یک مجموعه داده های شرکت متفاوت با سند مورد نوشتن و حاوی اطلاعات حساس باشد، قابل خواندن باشد. لذا اگر نقش واقعی یک مشاور شرکت کشاورزی i را در نظر بگیریم که هم اجازه خواندن و هم اجازه نوشتن روی اطلاعات حساس شرکت کشاورزی i را داشته باشد، آنگاه ماشین حالت و سلسله مراتب نقش های کارمند A به شکل 6 تغییر می‌کند.



شکل4-سلسله مراتب نقش ها ی کارمند A وماشین حالت آن



شکل5-سلسله مراتب نقش ها ی کارمند A وماشین حالت این سلسله مراتب پس از دسترسی بهi



شکل6-سلسله مراتب نقش ها ی کارمند A وماشین حالت این سلسله مراتب پس از دسترسی به i با در نظر گرفتن اجازه نوشتن