فصلنامه پژوهش‌های حفاظتی ـ امنیتی دانشگاه جامع امام حسین(علیه‌السلام)
سال سوم، شماره‌ی ۱۴ (تابستان ۱۳۹۴): صص ۴۷ – ۶۳

ارائه چارچوبی به منظور ارزیابی روش‌های کنترل دسترسی در فضای سایبر با تأثیر آن بر امنیت اطلاعات

محمد رشید نژاد[۱]
جمشید نصرت‌آبادی[۲]
محمد اقدسی[۳]

چکیده

با توجه به گستردگی و پیچیدگی حملات در فضای سایبر، روش‌ها و مدل‌های کنترل دسترسی به عنوان اولین راه‌حل مسئله امنیت اطلاعات در اشتراک‌گذاری اطلاعات در فضای سایبر توسعه‌یافته‌اند اما با وجود تحقیقات فراوان در این زمینه، تاکنون بررسی جامعی بر روی این مدل‌ها و روش‌ها صورت نگرفته است و معیارهای مشخصی برای ارزیابی این روش‌ها از لحاظ عملکرد و کارایی بازدارندگی آن‌ها و تأثیر مستقیم آن بر امنیت اطلاعات وجود ندارد. هدف این تحقیق تحلیل معیارهای کنترل دسترسی و تأثیر آن بر امنیت اطلاعات و ارائه معیارها و شاخص‌هایی برای ارزیابی مدل‌ها و روش‌های کنترل دسترسی به منظور اشتراک‌گذاری امن اطلاعات بین سازمانی در فضای سایبر است. این تحقیق با روش پیمایش و با یک بررسی جامع بر روی بیش از ۵۰ مدل و روش کنترل دسترسی در محیط به اشتراک‌گذاری امن اطلاعات در فضای سایبر انجام شده است. هم‌چنین معیارهایی برای ارزیابی و مقایسه این روش‌ها ارائه‌شده و می‌تواند پاسخگوی چالش امنیت در به اشتراک‌گذاری اطلاعات باشد که این معیارها ابتدا بر اساس مفاهیم و ویژگی‌های مدل‌ها و روش‌های کنترل دسترسی به دست آمد و سپس با استفاده از روش دلفی و اجماع نظر خبرگان موردبازنگری و تأیید قرار گرفت. بر این اساس سؤال اصلی تحقیق این است که چه معیارهایی از روش‌های کنترل دسترسی بر امنیت اطلاعات به اشتراک‌گذاری شده بین سازمان‌ها مؤثر است؟ نتایج این تحقیق نشان می‌دهد که روش‌های کنترل دسترسی لزوماً باعث افزایش امنیت نشده بلکه برخی از معیارها و عوامل در آن‌ها ازجمله انتشار اختیارات باعث کاهش امنیت اطلاعات به اشتراک‌گذاری شده می‌شود.

کلیدواژه‌ها: *امنیت اطلاعات، کنترل دسترسی، به اشتراک‌گذاری اطلاعات، چارچوب ارزیابی، فضای سایبری*

۱- کارشناس ارشد مهندسی فناوری اطلاعات دانشگاه تربیت مدرس security.org@gmail.com
۲- کارشناس ارشد مدیریت فناوری اطلاعات دانشگاه پیام نور تهران nosratabadi61@yahoo.com
۳- دکتری، هیئت‌علمی و دانشیار دانشگاه تربیت مدرس، دانشکده فنی و مهندسی aghdasim@modares.ac.ir

مقدمه

همکاری سازمان‌ها و شرکت‌ها در فضای سایبر و فعالیت‌های مرتبط با آن نیازمند به اشتراک‌گذاری داده‌ها، اطلاعات و منابع مختلف در یک محیط تعاملی است. در این بین یک ناسازگاری[1] و چالش مهم بین به اشتراک‌گذاری اطلاعات و امنیت آن مطرح می‌شود. (Zeng, Wang, Deng, Cao, & Khundker, 2012, pp. 545-556). با افزایش مقیاس به اشتراک‌گذاری داده‌ها، کنترل کاربری و دسترسی اطلاعات و خدمات بسیار پیچیده شده است. در فضای سایبری کاربران از دامنه‌ها و گروه‌های مختلف می‌توانند با انجام عملیاتی روی منابع به اشتراک‌گذاری شده، دسترسی داشته باشند. مشکل بنیادی امنیت در به اشتراک‌گذاری داده‌ها، کنترل مجوزها و تصدیق کاربران و مجوز دسترسی‌هایشان[2] برای نیل به منابع مبتنی بر مهارت یا وظیفه شغلی است (Lia, Zhangb, Xua, & Wua, 2009, pp. 260-275). بدین منظور محققان مختلف سعی بر رفع این مشکل با ارائه مدل و روش‌های مختلفی مانند کنترل دسترسی اختیاری و اجباری، کنترل دسترسی مبتنی بر نقش، کنترل دسترسی مبتنی بر گروه، کنترل دسترسی مبتنی بر وظیفه کرده‌اند (Gouglidis & Mavridis, 2012, pp. 540-556). این روش‌ها با سه مفهوم شناسایی، هویت سنجی و مجوز دهی همراه است. در تحقیقات مختلف تعدادی از مدل‌ها بر اساس معیارهایی مانند انعطاف‌پذیری، مقیاس‌پذیری، قابلیت استفاده، ریزدانگی، مدیریت اختیارات و انتشار اختیارات و ایمنی با یکدیگر مقایسه شده‌اند اما تاکنون چارچوب مناسبی برای ارزیابی روش‌های کنترل دسترسی بر اساس مفاهیم و ویژگی‌های آن‌ها و تأثیر آن‌ها بر امنیت اطلاعات ارائه نشده است. در این تحقیق معیارهای اصلی شناسایی و تعیین‌شده شامل مدیریت اختیارات، تخصیص اختیارات، انتشار اختیارات و ایمنی است که هر یک نیز به زیر مؤلفه‌هایی تقسیم می‌شود.

این تحقیق از نوع پیمایش بوده و اطلاعات در خصوص روش‌ها و مدل‌های کنترل دسترسی گردآوری‌شده و سپس با استفاده از روش دلفی به تحلیل و نتیجه‌گیری در مورد آن پرداخته‌شده است. نتایج این تحقیق می‌تواند به بهبود روش‌ها و مدل‌های کنترل دسترسی برای سازمان‌ها و سامانه‌ها کمک نموده تا در تصمیمات کنترل دسترسی در فضای سایبر و برقراری امنیت و دفاع سایبری، بتوانند تصمیم مناسبی را اتخاذ کنند.

1. Conflict
2. permission

۱- پیشینه تحقیق

موسسه NIST در سال ۲۰۱۴ چارچوبی را به منظور افزایش و بهبود امنیت اطلاعات زیرساخت‌های حیاتی کشور آمریکا در فضای سایبر ارائه نمود که در آن کنترل دسترسی به عنوان اولین مؤلفه حفاظتی و بازدارندگی معرفی‌شده است (NIST, 2014). کنترل دسترسی به منظور محدود کردن دسترسی کاربران، فرآیندها یا ابزارها به دارایی‌ها و تسهیلات متناظر برای انجام فعالیت‌ها و تراکنش‌های مجاز در این چارچوب تعریف می‌شود. به منظور داشتن یک روش کنترل دسترسی مؤثر، شناسه‌ها و حساب‌های کاربری برای کاربران و دستگاه‌های مجاز، کنترل فیزیکی به دارایی‌ها و کنترل از راه دور باید مدیریت و حفاظت شوند. هم‌چنین مجوزهای دسترسی بر اساس اصل کم‌ترین امتیاز دسترسی و تفکیک وظایف باید مدیریت شوند.

موسسه SANS نیز در نسخه پنجم کنترل‌های امنیتی حیاتی برای دفاع سایبری مؤثر که در سال ۲۰۱۴ منتشر کرده، مفهوم کنترل دسترسی را برای مؤلفه‌های حیاتی شبکه ازجمله لیست کنترل دسترسی در فایروال، روتر، سوییچ و ثبت رخدادهای مرتبط با هرگونه دسترسی به منابع شبکه و دسترسی‌های بدون مجوز، مانیتور کردن دسترسی‌ها برای تشخیص حملات در نظر گرفته است. هم‌چنین کنترل تجهیزات را با استفاده از سامانه کنترلی برای مدیریت متمرکز و تنظیم آن‌ها، طبقه‌بندی و اعطا مجوزهای دسترسی به داده‌ها و دارایی‌های شبکه پیشنهاد می‌کند (SANS, 2014).

۲- بیان مسئله، ضرورت و اهمیت آن و سؤالات تحقیق

به دلیل وجود روش‌های کنترل دسترسی متنوع در امنیت اطلاعات فضای سایبر، انتخاب یک روش مناسب برای سازمان‌ها به منظور امنیت اطلاعات به اشتراک‌گذاری شده بسیار مشکل است و چارچوب مناسب و کاربردی که بتوان به وسیله آن‌ها روش‌های کنترل دسترسی را مقایسه و درنهایت بهترین روش را انتخاب نمود وجود ندارد و این مسئله مدیران شبکه را در تصمیم‌گیری دچار تردید می‌نماید. در این تحقیق به بررسی روش‌های موجود برای حل این مسئله پرداخته‌شده است. هم‌چنین با توجه به اهمیت امنیت اطلاعات در عصر حاضر و رشد سریع و درعین‌حال نامتوازن ساختار فناوری اطلاعات انجام این تحقیق به بهبود روش‌ها و مدل‌های کنترل دسترسی برای سازمان‌ها و سامانه‌ها کمک نموده تا مدیران بتوانند به منظور برقراری امنیت اطلاعات در فضای سایبر، تصمیم مناسبی را اتخاذ کنند. وجود معیارهای ارزیابی و چارچوب مناسب برای ارزیابی آن‌ها می‌تواند کمک شایانی در تصمیم‌گیری سازمان‌ها و هم‌چنین

رشد و توسعه مناسب مدل‌ها و روش‌های کنترلی نماید. بر اساس این تحقیق با توجه به شناخت معیارهای روش‌های کنترل دسترسی که بر امنیت اطلاعات تأثیرگذار هستند، می‌توان با ارزیابی مدل‌های کنترل دسترسی در فضای سایبر، توان بازدارندگی یک روش و مدل کنترل دسترسی را در مقابل حملات و آسیب‌پذیری‌ها افزایش داده و نشت و افشای اطلاعات حساس و محرمانه سازمان‌ها را کاهش داد. بنابراین ضرورت ایجاب می‌نماید که با بررسی روش‌های مختلف در این حوزه به افزایش امنیت در به اشتراک‌گذاری اطلاعات کمک نمود.

بر این اساس سؤال اصلی تحقیق این است که چه معیارهایی از روش‌های کنترل دسترسی بر امنیت اطلاعات به اشتراک‌گذاری شده بین سازمان‌ها مؤثر است؟

۳- مروری بر اشتراک‌گذاری اطلاعات در فضای سایبر و چالش امنیت

همکاری[1] در فضای سایبر، مجموعه‌ای از فرایندها و خدمات است که سازمان‌ها برای دست‌یابی به یک هدف مشترک با یکدیگر تعامل و مشارکت دارند. در همکاری با خدمات و فرایندهایی روبرو هستیم که بین بخش‌های امنیتی متفاوت یا درون یک بخش صورت می‌گیرد و در جریان این همکاری یک خدمت با یک یا چندین خدمت تعامل دارد. در این تعاملات، عموماً خدمات از یکدیگر مجزا نیستند و ممکن است داده‌ها در یکسری از این خدمات جریان یابد و به اشتراک گذاشته شوند. در میان این تعامل، هر خدمت، نیاز به دسترسی به داده‌های خود داشته و اطلاعات موردنیاز خود را مبادله و وظایف مربوط به بخش خود را انجام می‌دهد (Altunay, Byrd, Brown, & Dean, 2008, pp. 547-554). ازاین‌رو خدماتی که نیاز به اطلاعات در فضای سایبر دارند باید بتوانند به نیازمندی‌های خود دست یابند و سایر اطلاعات نیز از دسترسی افراد و فرآیندهای غیرمجاز در امان باشند و با این اقدام به کاهش ریسک و به حداقل رساندن آسیب‌پذیری‌ها کمک نمایند.

در مسئله همکاری سازمانی و ارائه خدمات مشترک یک نگاه جامع و متعادل نسبت به مسئله امنیت و به اشتراک‌گذاری اطلاعات وجود ندارد. (Zeng, Wang, Deng, Cao, & Khundker, 2012, pp. 545-556). این بدین معنی است که گاهی برای رسیدن به امنیت بالا، اشتراک‌گذاری اطلاعات با سختی همراه شده و بالعکس برای رسیدن به دسترسی آسان به اطلاعات، سطح امنیت را کاهش می‌دهند. هدف اصلی امنیت اطلاعات محافظت از اطلاعات و سامانه‌های اطلاعاتی و کاهش ریسک مرتبط با سه هدف اصلی

1. Collaboration

محرمانگی، صحت و دسترسی‌پذیری است. کنترل دسترسی مانند مدیریت اجازه به منابع و سامانه‌ها یکی از مهم‌ترین مباحث پایه‌ای در امنیت اطلاعات و مکانیسم‌های امنیتی محسوب می‌شود (Fuchs, Pernu, & Sandhu, 2011, pp. 748-769).

٤- کنترل دسترسی راه‌حلی برای چالش امنیت در به اشتراک‌گذاری اطلاعات

خدمات جامع و انعطاف‌پذیر در محیط‌های عملیاتی بین شرکا و به اشتراک‌گذاری امن اطلاعات در فضای سایبر از مهم‌ترین مسائلی است که سازمان‌ها برای حل آن از روش‌ها و مدل‌های کنترل دسترسی استفاده می‌کنند (Sun, Gong, Meng, Lin, & Bertino, 2009, pp. 2629-2642). کنترل دسترسی روشن‌ترین نماد امنیت است. درواقع آن را قلب امنیت هم می‌دانند.

هم‌چنین برای به اجرا درآمدن اهداف محرمانگی، صحت و دسترس‌پذیری در بحث امنیت از نگاه سامانه مدیریت امنیت اطلاعات، این دامنه یک مبنا و پیش‌نیاز به‌حساب می‌آید. کنترل دسترسی برای تحقق سه هدف عمده به کار گرفته می‌شود که عبارت‌اند از:

۱- جلوگیری از دسترسی کاربران غیرمجاز به امکانات تغییر اطلاعات.

۲- جلوگیری از دست‌کاری اطلاعات به صورت غیر عمدی توسط کاربران ناآشنا و غیرمجاز.

۳- حصول اطمینان از سلامت اطلاعات و ثبات اطلاعات داخلی و خارجی.

این کنترل‌های دسترسی هستند که چگونگی و روش برقراری ارتباط بین کاربران و سامانه‌ها را تعیین کرده و به عبارتی دیگر با ایجاد محدودیت یا اعمال کنترل بر روی منابع اطلاعاتی شامل داده‌ها و یا سامانه‌ها از اطلاعات موجود در آن‌ها در برابر دسترسی‌های غیرمجاز محافظت می‌کنند.

روش‌ها و مدل‌های کنترل دسترسی، شکل و گستره دسترسی نهادها (کاربران یا فرآیندها) به اشیاء (منابع اطلاعاتی) را مدیریت می‌نماید. در حقیقت در مدل کنترل دسترسی نحوه اعطا امتیازات و مجوزهای دسترسی و لغو آن‌ها تعیین می‌شود.

مسئله حساب کاربری و مجوز دسترسی در به اشتراک‌گذاری اطلاعات در فضای سایبر بسیار مهم است و با مواردی همچون استفاده غیرمجاز بعد از لغو دسترسی، حذف نشدن دسترسی‌ها، تحمیل هزینه مازاد به مدیر سامانه در تعریف کنترل دسترسی روبه‌رو است.

تحقیقات در خصوص مدل‌های کنترل دسترسی در دهه‌های ۱۹۶۰و ۱۹۷۰ آغازشده است. در این سال‌ها دو مدل کنترل دسترسی اختیاری[1] و کنترل دسترسی اجباری[2] مطرح شد. مدل کنترل دسترسی اختیاری، کنترل دسترسی را بر اساس درخواست‌کننده و قواعد دسترسی صریح که بیان می‌کنند چه کسی مجاز به انجام چه عملی روی چه منبعی است، اعمال می‌کنند. در این مدل به کاربرانش اجازه داده می‌شود تا بر اساس اختیار خود، دسترسی‌هایشان را بدون نیاز به دخالت مدیر سامانه، برای دیگر کاربران به صورت وکالتی بفرستند.

در مدل کنترل دسترسی اجباری، سه مفهوم مطرح است:

اشیایی[3] (منابع اطلاعاتی) که قرار است محافظت شوند. نهادهایی (کاربر یا فرآیند و...)که قرار است روی اشیاء فعالیت‌هایی انجام دهند. عملیاتی[4] که می‌توانند روی اشیاء اجرا شوند و باید کنترل شوند. در این مدل یک واحد صلاحیت مرکزی دسترسی‌ها را کنترل می‌کنند و می‌توان جریان اطلاعات بین اشیا و نهادها را نیز توسط تنظیمات این واحد کنترل کرد (Fuchs, Pernu, & Sandhu, 2011, pp. 748-769).

این دو مدل، روش‌های سنتی در کنترل دسترسی محسوب می‌شوند که در محیط‌های متمرکز کاربرد داشتند. نکته مهم این است که این روش‌های سنتی کنترل دسترسی اجباری و اختیاری در محیط‌های تعاملی که اصولاً غیرمتمرکز و دائماً در حال تغییرند، مناسب نیستند. ازاین‌رو مدل کنترل دسترسی مبتنی بر نقش که انعطاف‌پذیرتر و در محیط‌های پویا کاربردی‌تر است، طراحی شد. پاولیچ و همکارانش در سال ۲۰۱۰ به بررسی این مدل‌ها و مفاهیم اصلی شیء، نهاد، مجوز دسترسی، سلسله‌مراتب دسترسی، وکالت و نقش سروکار دارند، پرداخته‌اند (Pavlich-Mariscal, Demurjian, & Michel, 2010, pp. 350-379). این مدل‌ها از این جهت مهم هستند که محدوده وسیعی از نیازمندی‌های کنترل دسترسی را پوشش می‌دهند و پایه اکثر مدل‌های کنترلی هستند.

مدل کنترل دسترسی اجباری در جاهایی که حفاظت از اطلاعات و امنیت از اهمیت بالاتری برخوردار است، مورداستفاده قرار می‌گیرد. و مدل اختیاری پاسخ‌گوی مناسب‌تری برای محیط‌های پویا و تعاملی[5] است.

1. Discretionary Access control (DAC)
2. Mandatory Access control (MAC)
3. Subject
4. Operations
5. collaborative and dynamic

مدل کنترل دسترسی مبتنی بر نقش برای سازمان‌هایی که وظایف و مجوزهای دسترسی کارکنانش متناظر با جایگاه آن در سازمان تغییر می‌کند و این تغییرات زیاد تکرار می‌شود، مناسب‌تر هستند.

۵- مروری بر روش‌های مقایسه و ارزیابی مدل‌های کنترل دسترسی

محققان و مؤسسات مختلف با رویکردهای خاص و متمایزی تعداد اندکی از مدل‌ها و روش‌های کنترل دسترسی را با یکدیگر مقایسه نموده یا شاخص‌هایی را برای اندازه‌گیری صحت عملکرد آن‌ها ارائه داده‌اند. درنتیجه این معیارها نمی‌تواند چارچوب مناسبی برای مقایسه و ارزیابی غالب روش‌های کنترل دسترسی و از همه مهم‌تر تأثیر آن بر امنیت اطلاعات به اشتراک‌گذاری شده باشد.

موسسه ملی تکنولوژی و استاندارد آمریکا (NIST) در سال ۲۰۱۲ راهنمایی را برای معیار اندازه‌گیری سامانه کنترل دسترسی ارائه کرد (Hu & Scarfone, 2012). در این راهنما، به شاخص‌هایی نیز برای ارزیابی یک سامانه کنترل دسترسی اشاره شده است. این راهنما به چهار ویژگی مدیریت، اجرا، کارایی و پشتیبانی تقسیم شده است که دو ویژگی مدیریت و اجرا با تأثیرگذاری بر کارایی و عملکرد مدل، مدنظر قرارگرفته است. در ویژگی مدیریت، فاکتورهای سادگی در تخصیص اختیارات و توانایی وکالت در سطح بین مدیریتی و در ویژگی اجرا، فاکتورهای پشتیبانی از اصل کم‌ترین امتیاز دسترسی، تفکیک وظایف، ایمنی (قیود و محدودیت‌ها)، جلوگیری از تضاد، ریزدانگی در کنترل و ویژگی وضوح مدل مدنظر است.

سادگی در تخصیص مجوزها شامل گام‌های کمتر موردنیاز برای تخصیص، تغییر، لغو نهاد[1] و مجوزهای آن‌ها بر اساس تغییرات در ساختار یا مسئولیت‌ها است. به‌عنوان‌مثال در مدل کنترل دسترسی مبتنی بر نقش، نهاد به نقش تخصیص می‌یابد و نقش دارای مجوز است. هم‌چنین نقش‌ها بر اساس مسئولیت و صلاحیت در سازمان ایجاد و تخصیص می‌یابد و نهاد با تغییر جایگاه سازمانی خود، به راحتی نقش قبلی را لغو و نقش جدید را به دست می‌آورد. وجود سلسله‌مراتب و ارث‌بری یک نهاد در مجوزهای دسترسی از گروهی که عضو آن است، باعث افزایش سادگی در استفاده می‌شود. تضاد در سیاست‌ها می‌تواند نتیجه یک بن‌بست در دسترسی به دلیل وابستگی در قوانین مربوطه باشد یا به دلیل تضاد در بین چند سیاست دسترسی در تصمیم‌گیری اعطا یا تخصیص دسترسی ایجاد شود. وجود ویژگی جلوگیری از تضاد در یک مدل باعث افزایش امنیت مدل است.

1. object

حسنی و مدیری نیز در سال ۲۰۱۳ مشخصاتی را برای مقایسه و ارزیابی مدل‌های کنترل دسترسی ارائه کردند که شامل مقیاس‌پذیری، انعطاف‌پذیری، سطح کارایی، وضوح، مدیریت اختیارات و دسترسی، قیود، وکالت، صفات، ریزدانگی و زمینه است (Hasani & Modiri, 2013). سان و همکارانش در بررسی ویژگی‌های سیاست امنیتی انعطاف‌پذیر در یک همکاری فعال به رویکردهای مختلف محققان در تدوین و خلق مدل‌های کنترل دسترسی اشاره‌کرده‌اند. در تحقیق آن‌ها به معیارهایی ازجمله مدیریت اختیارات، سلسله‌مراتب دسترسی، تخصیص خودکار اختیارات و قیود اشاره شده است. (Sun, Gong, Meng, Lin, & Bertino, 2009). محققان دیگری مانند ژائو و همکارانش نیز در هنگام ارائه مدل کنترل دسترسی همکاری، برخی روش‌های کنترل دسترسی را با یکدیگر از لحاظ سازگاری با تغییرات، وضوح، سادگی در استفاده، سادگی در مدیریت و پشتیبانی از حقوق دسترسی جدید مقایسه نمودند (Zhao, 2001).

همان‌گونه که مشخص است این معیارها و روش‌های ارزیابی، فقط برای شرایط خاص توسط محقق طرح‌ریزی شده و روی چند مدل قابل پیاده‌سازی است و این در حالی است که برای غالب روش‌ها و مدل‌های کنترل دسترسی قابل‌اعمال نیستند و هر یک دارای نقاط ضعف و قوت خود هستند. لذا برای مقایسه یا ارزیابی مدل‌های کنترل دسترسی و تأثیر آن بر امنیت اطلاعات باید چارچوب جامع‌تری را طراحی نمود که زوایای مختلف مدل‌ها را بررسی کند.

٦- معیارهای اصلی روش‌های کنترل دسترسی

بر اساس مرور تحقیقات پیشین و بررسی بیش از ۵۰ مدل و روش کنترل دسترسی، معیارهای اصلی و پایه‌ای این مدل‌ها برای ایجاد امنیت و نقش این معیارها در افزایش و کاهش امنیت، از آن‌ها استخراج شد. نمونه‌ای از این مدل‌ها شامل کنترل دسترسی اجباری، اختیاری (Fuchs, Pernu, & Sandhu, 2011, pp. 748-769) و (Pavlich-Mariscal, Demurjian, & Michel, 2010, pp. 350-379)، لیست کنترل دسترسی (Zhang & Parashar, 2006, pp. 19-27)، کنترل دسترسی مبتنی بر نقش (Sandhu, Coyne, Reinstein, & Youman, 1996, pp. 38-47)، مبتنی بر نقش سلسله‌مراتبی، مبتنی بر نقش قید دار، مبتنی بر نقش متقارن (Zhao, 2001)، کاربر–نقش اجرایی، چارچوب ترکیب سیاست، مبتنی بر نقش گروه مبنا (Li, Zhang, Xu, & Wu, 2009, pp. 260-275)، مبتنی بر نقش دامنه‌ای (Gouglidis & Mavridis, 2012, pp. 540-556)، مبتنی بر نقش افزایشی (Le, Doll, Barbosu, Luque, & Wang, 2012)، مبتنی بر حاشیه (Nasirifard, Peristeras, & Decker, 2011, pp. 1352-1364)، مبتنی بر سیاست سازمانی (Kalama, Deswarteb, Baïnab, & Kaânicheb, 2009, pp. 154-

(169، چارچوب مبتنی بر نقش و ریسک (Hu, Li, Lu, Lu, & Ma, 2011, pp. 574-586)، مبتنی بر فعالیت – وظیفه (Lu, Zhang, & Sun, 2009, pp. 403-415)، مبتنی بر نقش مورد اعتماد (Zhi-gang, Zheng-ding, Rui-xuan, Wei, & Xiao-gang, 2004, pp. 694-698)، زیرساخت مدیریت امتیازات (Shaomin, Baoyi, & Lihua, 2006, pp. 1827-1830)، کنترل دسترسی مبتنی بر سازمان (Kalama, Deswarteb, Baïnab, & Kaânicheb, 2009, pp. 154-169) و (Preda, Cuppens, Cuppens-Boulahia, Garcia-Alfaro, & Toutain, 2011, pp. 1144-1159)، کنترل دسترسی توسعه‌یافته (Ben-Ghorbel-Talbi, Cuppens, Cuppens-Boulahia, & Bouhoula, 2010, pp. 209-236)، کنترل دسترسی مبتنی بر تیم و کنترل دسترسی مبتنی بر تیم – زمینه (Essmayr, Probst, & Weippl, 2004, pp. 127-156) و (Demirkan & Goul, 2013, pp. 51-91)، کنترل دسترسی تیم مبتنی بر زمینه، کنترل اختیارات مبتنی بر وظیفه، کنترل دسترسی زمینه آگاه (Demirkan & Goul, 2013)، مبتنی بر محتوا، مبتنی بر نقش تعمیم‌یافته، مبتنی بر نقش پویا (Zhang & Parashar, 2006, pp. 19-27)، مبتنی بر وظیفه و نقش، مبتنی بر شیء (Essmayr, Probst, & Weippl, 2004, pp. 127-156)، مبتنی بر صفت (Lang, Foster, Siebenlist, Ananthakrishnan, & Freeman, 2009, pp. 169-180) و (Zhu & Smari, 2008, pp. 31-35)، سیاست چندگانه مبتنی بر صفت (Lang, Foster, Siebenlist, Ananthakrishnan, & Freeman, 2009, pp. 169-180)، مبتنی بر گزاره (Wu, Sheth, Miller, & Luo, 2002, pp. 71-94)، مشترک (Ma, Lu, & Qiu, 2010, pp. 699-717) و کنترل دسترسی فعالیت گرا (Le, et al., 2010, pp. 2979-2990) و مبتنی بر تعامل (Altunay, Byrd, Brown, & Dean, 2008, pp. 547-554) است.

معیارهای اصلی شامل معیارهایی است که یک مدل کنترل دسترسی باید بر اساس آن توسعه یابد (Hasani & Modiri, 2013, pp. 19-29). متناسب با محورهای توسعه، معیارهای مختلفی نیز بر اساس مرور تحقیقات انجام شده به دست آمد و پس از قرار دادن این معیارها در کنار یکدیگر و دسته‌بندی[1] آن‌ها با توجه به نوع عملکرد، ماهیت هر معیار و کاربرد آن، به چهار دسته تقسیم شدند.

معیارهای اصلی استخراج‌شده پس از تحلیل روش‌های کنترل دسترسی شامل دسته‌بندی زیر است:

۱- مدیریت اختیارات

۲- تخصیص اختیارات

۳- انتشار اختیارات

۴- ایمنی

1. cluster

مدیریت اختیارات شامل مدیریت متمرکز، غیرمتمرکز و ترکیبی است. ۶ مدل مدیریت اختیارات غیرمتمرکز، ۲۷ مدل مدیریت اختیارات متمرکز و ۱۷ مدل نیز مدیریت اختیارات ترکیبی دارند.

تخصیص اختیارات شامل تخصیص پویای اختیارات، تخصیص اختیارات مبتنی بر زمینه، صفات و اعتماد است. ۹ مدل تخصیص اختیارات پویا، ۱۵ مدل تخصیص مبتنی بر زمینه، ۸ مدل مبتنی بر صفات، ۴ مدل مبتنی بر وظیفه و ۶ مدل مبتنی بر اعتماد بودند.

انتشار اختیارات شامل سلسله‌مراتب دسترسی، وکالت و نگاشت نقش است. ۱۶ مدل از سلسله‌مراتب دسترسی در مدل خود پشتیبانی می‌کنند. ۸ مدل از وکالت و ۳ مدل نیز از مفهوم نگاشت نقش پشتیبانی کرده‌اند.

ایمنی شامل پشتیبانی از قیود ازجمله قید تفکیک وظایف و قید زمینه، اصل کم‌ترین امتیاز دسترسی و جلوگیری از تضاد سیاست‌های دسترسی است. ۴۰ مدل اصل کم‌ترین امتیاز دسترسی را به عنوان یک معیار امنیتی در مدل خود در نظر گرفته‌اند. ۷ مدل از قید تفکیک وظایف و ۱۰ مدل از زمینه به عنوان قید و عامل محدودیت استفاده کرده‌اند. ۴ مدل نیز از معیار جلوگیری از تضاد سیاست‌ها برای امنیت مدل استفاده کرده‌اند.

۷- تجزیه و تحلیل

در این تحقیق، تحلیل و اعتبارسنجی معیارهای اصلی و تأثیر آن‌ها بر کارایی و عملکرد به اشتراک‌گذاری اطلاعات و امنیت آن در فضای سایبر صورت گرفته و سپس با استفاده از روش دلفی و اجماع نظر خبرگان تحلیل‌شده و در انتها چارچوبی برای ارزیابی و انتخاب روش‌ها پیشنهادشده است. تحقیق حاضر یک چارچوب کلی و کیفی را برای انتخاب روش‌های کنترل دسترسی ارائه می‌دهد و برای این‌که بتوان این روش‌ها را دو به دو باهم مقایسه و ارزیابی نمود باید مدل‌های مختلفی را مبتنی بر این چارچوب طراحی کرد و هر یک از معیارها را بر اساس محیط اجرایی، وزن دهی و کمی سازی نمود که تحقیقات جداگانه‌ای را می‌طلبد.

ابتدا با تحلیل معیارها از نظر درستی و قابل اعتبار بودن، چارچوبی برای ارزیابی برگرفته از معیارهای استخراج‌شده و تأثیر آن‌ها بر امنیت ارائه‌شده است. سپس این چارچوب از نظر صحت و درستی مورد تأیید و ارزیابی قرارگرفته که برای این منظور از روش دلفی استفاده گردید. در فرایند دلفی، چارچوب پیشنهادی نخست به صورت پرسشنامه با سؤالات کیفی تهیه و در اختیار خبرگان و متخصصان قرار گرفت که به منظور روایی پرسشنامه در اولین گام برخی از سؤالات موردبازنگری و اصلاح قرار گرفت سپس طی دو مرحله نظرات

خبرگان در مورد معیارهای ارزیابی و تأثیر آن‌ها بر یکدیگر و امنیت در به اشتراک‌گذاری اطلاعات در فضای سایبر جمع‌آوری گردید و اطلاعات جمع‌آوری‌شده از خبرگان توسط محققان تجزیه و تحلیل گردیدند که در مرحله اول فرایند دلفی ۳۰٪ از پاسخ‌های جمع‌آوری‌شده اجماع نظر و همگرایی لازم را نداشتند که به منظور همگرایی حداکثری در مرحله دوم سایر پرسش‌ها اصلاح گردیده و پس‌ازاین مرحله اجماع نظر خبرگان به دست آمد و چارچوب پیشنهادی تأیید و نهایی گردید. با توجه به نوع تحقیق می‌باید از افراد خبره در این حوزه استفاده می‌گردید. لذا ۱۰ نفر از متخصصان و افراد خبره در حوزه‌های مختلف امنیت اطلاعات، معماری فرآیندها، تحلیل سامانه‌ها، برنامه‌نویسی و شبکه با سمت‌های مختلف مدیریتی و کارشناسی در سازمان فناوری اطلاعات نیروهای مسلح همکاری نمودند. در جدول ۱ مشخصات عمومی و تخصصی این افراد نشان داده‌شده است. افراد انتخاب‌شده در چندین حوزه فعالیت و تخصص دارند.

جدول ۱: ویژگی خبرگان انتخابی برای روش دلفی

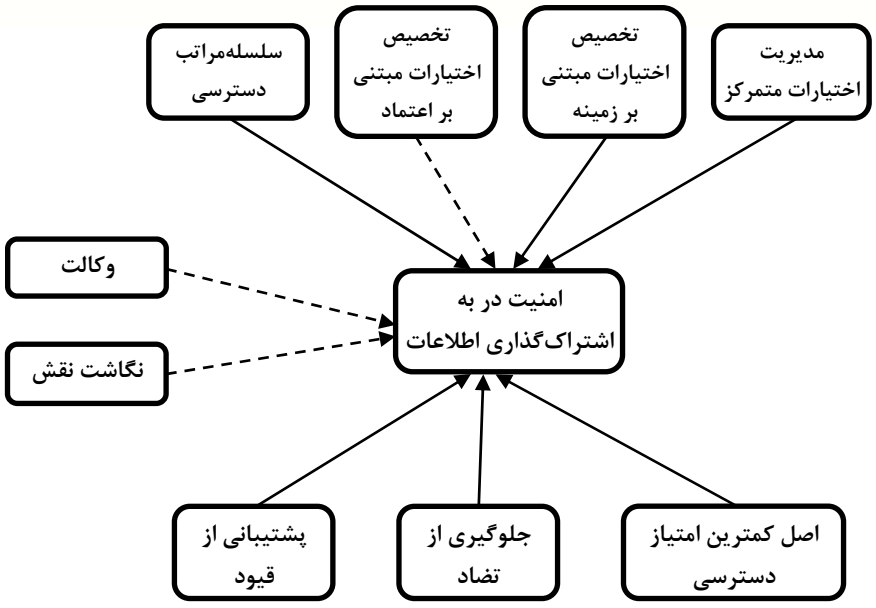
محدوده سنی	۳۰ ـ ۴۵ سال	۱۰
سابقه فعالیت تخصصی	۱۰ ـ ۲۵ سال	۱۰
تحصیلات	دکترا	۳
	کارشناسی ارشد	۳
	کارشناسی	۴
رشته تحصیلی	دکترا ـ مدیریت فناوری اطلاعات	۳
	کارشناسی ارشد ـ مهندسی نرم‌افزار	۱
	کارشناسی ارشد ـ مدیریت فناوری اطلاعات	۱
	کارشناسی ارشد ـ امنیت اطلاعات	۱
	کارشناسی ـ مهندسی سخت‌افزار	۴
سمت	مدیر	۴
	کارشناس	۶
تخصص/ خبرگی افراد به تفکیک	تولید برنامه‌های کاربردی	۵
	تحلیل سامانه‌ها	۴
	امنیت اطلاعات	۵
	شبکه‌های رایانه‌ای	۳
	تحلیل و معماری فرآیندها	۲
	مدیریت مجوزهای دسترسی در سطح شبکه و برنامه‌های کاربردی	۷
	مدیریت راهبردی سامانه‌های اطلاعاتی	۴

پس از بررسی و اجماع نظرات متخصصان در خصوص معیارهای ارزیابی و تأثیر آن بر افزایش یا کاهش امنیت، نتایج زیر به دست آمد:

معیارهای اصلی که برای ارزیابی ارائه می‌گردد شامل مدیریت اختیارات (متمرکز/غیرمتمرکز/ترکیبی)، تخصیص اختیارات (مبتنی بر زمینه/اعتماد)، انتشار اختیارات (وکالت/نگاشت نقش/سلسله‌مراتب دسترسی) و ایمنی (پشتیبانی از قیود/جلوگیری از تضاد سیاست دسترسی) است. تأثیر معیارهای اصلی مدل کنترل دسترسی بر اشتراک‌گذاری امن اطلاعات زمانی است که به صورت ترکیبی استفاده گردد. به‌عنوان‌مثال مدیریت اختیارات متمرکز در صورت تأثیر مثبت که بر امنیت دارد به صورت مناسب و همراه با سلسله‌مراتب دسترسی و وکالت پیاده‌سازی گردد.

یک روش کنترل دسترسی زمانی به بلوغ خود در به اشتراک‌گذاری امن اطلاعات می‌رسد که بسته به محیط مورداستفاده در فضای سایبر و نیازمندی‌های آن از معیارهای اصلی ترکیبی به صورت هم‌زمان پشتیبانی کند. در حقیقت اگر معیاری در مدل استفاده می‌شود که باعث کاهش امنیت می‌شود باید به صورت ترکیبی از معیاری که باعث افزایش امنیت می‌شود، استفاده نمود. به‌عنوان‌مثال تخصیص اختیارات مبتنی بر اعتماد و یا نگاشت نقش زمانی باعث افزایش امنیت می‌شود که با قیود ترکیب شود.

به منظور استفاده از این چارچوب برای ارزیابی روش‌های کنترل دسترسی یا حتی طراحی این روش‌ها، باید فاکتورهای موجود در این مدل را با چارچوب مقایسه نمود که در صورت داشتن این فاکتورها می‌توان به صورت کیفی، ارزیابی مناسبی را انجام داد. بر اساس معیارهای احصا شده از مرور تحقیقات و ویژگی روش‌های کنترل دسترسی، معیارهای زیر به صورت متغیرهای مستقل و وابسته در قالب چارچوب پیشنهادی شکل ۱ برای ارزیابی روش‌های کنترل دسترسی ارائه گردید:



شکل ۱: چارچوب پیشنهادی ارزیابی روش‌های کنترل دسترسی

خطوطی که با نقطه‌چین نشان داده‌شده است باعث کاهش تأثیرگذاری بر امنیت اطلاعات و خطوطی که با خط پر نشان داده‌شده، باعث افزایش تأثیرگذاری بر امنیت اطلاعات می‌شود.

نتیجه‌گیری

این تحقیق، دید جامعی از مدل‌های کنترل دسترسی و مفاهیم آن در به اشتراک‌گذاری امن اطلاعات در فضای سایبر به وجود می‌آورد. نتایج تحقیق نشان‌دهنده این واقعیت است که با وجود این‌که کنترل دسترسی برای ایجاد امنیت طراحی‌شده اما استفاده از یک روش کنترل دسترسی لزوماً باعث افزایش امنیت نمی‌شود بلکه برخی از معیارها و عوامل در آن‌ها ازجمله انتشار اختیارات و یا عدم استفاده از آن معیارها باعث کاهش امنیت اطلاعات به اشتراک‌گذاری شده و ایجاد حفره‌های امنیتی ناخواسته می‌شود. چارچوب پیشنهادی با رویکرد افزایش امنیت در به اشتراک‌گذاری اطلاعات می‌تواند به تصمیم‌گیری سازمان‌ها برای انتخاب روش کنترل دسترسی مناسب کمک کند.

بر اساس چارچوب پیشنهادی، مدیریت اختیارات متمرکز، تخصیص اختیارات مبتنی بر زمینه، سلسله‌مراتب دسترسی، اصل کم‌ترین امتیاز دسترسی، جلوگیری از تضاد و پشتیبانی از قیود در روش کنترل

دسترسی باعث افزایش امنیت در به اشتراک‌گذاری اطلاعات و تخصیص اختیارات مبتنی بر اعتماد، وکالت و نگاشت نقش باعث کاهش امنیت در به اشتراک‌گذاری اطلاعات می‌گردد. معیارهای موجود در چارچوب پیشنهادی، دید مناسبی را برای طراحان و استفاده‌کنندگان از مدل‌های کنترل دسترسی به وجود می‌آورد. هم‌چنین برای استفاده از این چارچوب باید به محیط بهره‌برداری در فضای سایبر و نیازمندی‌های آن محیط توجه نمود. در به اشتراک‌گذاری امن اطلاعات، ترکیبی از معیارهای اصلی و قرار دادن آن‌ها در کنار یکدگر باعث حفظ کارایی و اثربخشی روش کنترل دسترسی می‌شوند. با استفاده از چارچوب پیشنهادی می‌توان مدل‌ها و روش‌های کنترل دسترسی را ارزیابی و مدل مناسب را انتخاب نمود و سپس بر اساس آن امنیت در به اشتراک‌گذاری اطلاعات در فضای سایبر را ارتقا داده و باعث کاهش آسیب‌پذیری‌ها و جلوگیری از نشت و افشای اطلاعات حساس و محرمانه سازمان‌ها گردید.

منابع:

Altunay, M., Byrd, G. T., Brown, D. E., & Dean, R. A. (2008). An Interaction-based Access Control Model (IBAC) for Collaborative Services. ***Collaborative Technologies and Systems International Symposium***, (pp. 547 - 554). Irvine.

Ben-Ghorbel-Talbi, M., Cuppens, F., Cuppens-Boulahia, N., & Bouhoula, A. (2010). A delegation model for extended RBAC. ***Int. J. Inf. Secur.Springer-Verlag, 9***, 209–236.

Demirkan, H., & Goul, M. (2013). Taking value-networks to the cloud services: security services, semantics and service level agreements. ***Inf Syst E-Bus Manage.Springer-Verlag***, 51–91.

Essmayr, W., Probst, S., & Weippl, E. (2004). Role-Based Access Controls: Status, Dissemination ,and Prospects for Generic Security Mechanisms. ***Electronic Commerce Research, 4***, 127–156.

Fuchs, L., Pernu, G., & Sandhu, R. (2011). Roles in information security - A survey and classification of the research area. ***Computers & Security, 30,*** 748-769.

Gouglidis, A., & Mavridis, I. (2012). domRBAC: An access control model for modern collaborative systems. ***Computers & Security, 31,*** 540-556.

Hasani, S. M., & Modiri, N. (2013). Criteria Specifications for the Comparison and Evaluation of Access Control Models. ***I. J. Computer Network and Information Security, 5,*** 19-29.

Hu, J., Li, R., Lu, Z., Lu, J., & Ma, X. (2011). RAR: A role-and-risk based flexible framework for secure collaboration. ***Future Generation Computer Systems, 27,*** 574–586.

Hu, V. C., & Scarfone, K. (2012). ***Guidelines for Access Control System Evaluation Metrics***. National Institute of Standards and Technology (NIST).

Kalama, A. A., Deswarteb, Y., Baïnab, A., & Kaânicheb, M. (2009). PolyOrBAC: A security framework for Critical Infrastructures. ***INTERNATIONAL JOURNAL OF CRITICAL INFRASTRUCTURE PROTECTION, 2,*** 154-169.

Lang, B., Foster, I., Siebenlist, F., Ananthakrishnan, R., & Freeman, T. (2009). A Flexible Attribute Based Access Control Method for Grid Computing. ***J Grid Computing, 7,*** 169–180.

Le, X. H., Doll, T., Barbosu, M., Luque, A., & Wang, D. (2012). An enhancement of the Role-Based Access Control model to facilitate information access management in context of team collaboration and workflow. ***Journal of Biomedical Informatics, 45,*** 1084-1107.

Le, X. H., Lee, S., Lee, Y.-K., Lee, H., Khalid, M., & Sankar, R. (2010). Activity-oriented access control to ubiquitous hospital information and services. ***Information Sciences, 180,*** 2979–2990.

Li, Q., Zhang, X., Xu, M., & Wu, J. (2009). Towards secure dynamic collaborations with group-based RBAC model. ***Computers & Security, 28,*** 260-275.

Lia, Q., Zhangb, X., Xua, M., & Wua, J. (2009). Towards secure dynamic collaborations with group-based RBAC model. ***Computers & Security, 28,*** 260-275.

Lu, Y., Zhang, L., & Sun, J. (2009). Task-activity based access control for process collaboration environments. ***Computers in Industry, 60,*** 403–415.

Ma, C.-h., Lu, G.-d., & Qiu, J. (2010). An authorization model for collaborative access control. ***Journal of Zhejiang University-SCIENCE C (Computers & Electronics), 11,*** 699-717.

Nasirifard, P., Peristeras, V., & Decker, S. (2011). Annotation-based access control for collaborative information spaces. ***Computers in Human Behavior, 27,*** 1352–1364.

NIST. (2014). ***Framework for Improving Critical Infrastructure Cybersecurity***. National Institute of Standards and Technology.

Pavlich-Mariscal, J. A., Demurjian, S. A., & Michel, L. D. (2010). A framework of composable access control features:Preserving separation of access control concerns from models to code. ***Computers & Security, 29,*** 350-379.

Preda, S., Cuppens, F., Cuppens-Boulahia, N., Garcia-Alfaro, J., & Toutain, L. (2011). Dynamic deployment of context-aware access control policies for constrained security devices. ***The Journal of Systems and Software, 84,*** 1144–1159.

Sandhu, R., Coyne, E., Reinstein, H., & Youman, C. (1996). Role-based access control model. ***IEEE Computer, 29***(2), 38–47.

SANS. (2014). ***The Critical Security Controls for Effective Cyber Defense-Version 5.0.*** SANS Institute.

Shaomin, Z., Baoyi, W., & Lihua, Z. (2006). A Cache Considering Role-Based Access Control and Trust in Privilege Management Infrastructure. ***Wuhan University Journal of Natural Sciences, 11***(6), 1827-1830.

Sun, Y., Gong, B., Meng, X., Lin, Z., & Bertino, E. (2009). Specification and enforcement of flexible security policy for active cooperation. ***Information Sciences, 179***, 2629–2642.

Wu, S., Sheth, A., Miller, J., & Luo, Z. (2002). Authorization and Access Control of Application Data in Workflow Systems. ***Journal of Intelligent Information Systems, 18***, 71-94.

Zeng, Y., Wang, L., Deng, X., Cao, X., & Khundker, N. (2012). Secure collaboration in global design and supply chain environment: Problem analysis and literature review. ***Computers in Industry, 63,*** 545–556.

Zhang, G., & Parashar, M. (2006). SESAME: Scalable, Environment Sensitive Access Management Engine. ***Cluster Computing Springer Science, 9,*** 19–27.

Zhao, B. (2001). Collaborative Access Control. ***Seminar on Network Security 2001.***

Zhi-gang, W., Zheng-ding, L., Rui-xuan, L., Wei, W., & Xiao-gang, W. (2004). TrustedRBAC- A Distributed Authorization Infrastructure Span Multiple Autonomous Domains. ***Wuhan University Journal of Natural Sciences, 9***(5), 694-698.

Zhu, J., & Smari, W. W. (2008). Attribute Based Access Control and Security for Collaboration Environments. ***Aerospace and Electronics Conference IEEE National,*** (pp. 31 - 35). Dayton.