Journal of Soft Computing and Information Technology (JSCIT)
Babol Noshirvani University of Technology, Babol, Iran
Journal Homepage: jscit.nit.ac.ir
Volume 11, Number 2, Summer 2022, pp. 76-90
Received: 04/04/2022, Revised: 08/30/2022, Accepted: 09/18/2022

Improving the Self-adaptive Authorization Framework and solve its cold start problem using the concept of trust and I-sharing

Elham Moeinaddini[1] and Eslam Nazemi[2*]
1- Faculty of Computer Engineering and Science, Shahid Beheshti University, Tehran, Iran.
2*- Faculty of Computer Engineering and Science, Shahid Beheshti University, Tehran, Iran.
[1] e_moeinaddini@sbu.ac.ir and [2*]nazemi@sbu.ac.ir

Corresponding author's address: Eslam Nazemi, Shahid Beheshti University, Shahid Shahriari Square, Evin, Tehran, Iran.

Abstract- Authorization systems are an important part of security systems that are responsible for protecting resources. With the increasing number of users in organizations, managing the authorization infrastructure has become increasingly time-consuming and error-prone and misconfiguration of policies has reduced the effectiveness of these systems. Researchers recommend dynamic access control methods as an effective way to issue licenses in these systems. Since the sources of decision making in these methods are the defined policies and user records, there are no special restrictions for new users and these methods face the problem of cold start. In this paper, to solve this limitation, the concepts of trust and I-sharing are used, and a new method for improving the Self-Aaptive Authorization Framework (SAAF) called ISAAF is presented. ISAAF is a framework for self-adaptive control of authorization systems using the MAPE-K autonomous reference model, which estimates the trust of new users using the trust of users with whom they have common features. I-sharing groups, which include similar users are formed according to the role and identity features of users, using K-means clustering. Utilizing the concepts of trust and I-Sharing and grouping users by using their role and identity features is proposed for the first time in this paper and the experimental results indicate that the proposed method compared to other similar methods, produces better results in terms of accuracy of identifying malicious users and reducing their activity time in the system. Another advantage of this method is the implementation of MAPE-K loop elements and users using agents, which makes the system more independent and flexible. Compared to SAAF, ISAAF has reduced malicious users detection time by an average of 55 percent and improved detection accuracy of malicious users by more than 7 percent.

Keywords- Self-Adaptive Authorization Framework, Trust, Cold Start, Insider Threats, I-Sharing.

مجله علمی پژوهشی رایانش نرم و فناوری اطلاعات
دانشگاه صنعتی نوشیروانی بابل
صفحه مجله: jscit.nit.ac.ir
جلد ۱۱، شماره ۲، تابستان ۱۴۰۱ ، صفحه ۷۶-۹۰
دریافت: ۱۴۰۱/۰۱/۱۵، بازنگری: ۱۴۰۱/۰۶/۰۸ ، پذیرش: ۱۴۰۱/۰۶/۲۷

بهبود چارچوب مجوز خودتطبیق و حل مشکل شروع سرد آن با استفاده از مفهوم اعتماد و I-sharing

الهام معین‌الدینی[۱] و اسلام ناظمی*[۲]
۱- دانشکده مهندسی و علوم کامپیوتر، دانشگاه شهید بهشتی، تهران، ایران.
*۲- دانشکده مهندسی و علوم کامپیوتر، دانشگاه شهید بهشتی، تهران، ایران.
[1] e_moeinaddini@sbu.ac.ir and [2*]nazemi@sbu.ac.ir

* نشانی نویسنده مسئول: اسلام ناظمی، تهران، اوین، میدان شهید شهریاری، دانشگاه شهید بهشتی، دانشکده مهندسی و علوم کامپیوتر.

چکیده- سیستم‌های مجوز بخش مهمی از سیستم‌های امنیتی محسوب می‌شوند که وظیفه حفاظت از منابع را به‌عهده‌دارند. با افزایش کاربران در سازمان‌ها، مدیریت زیرساخت‌های صدور مجوز به‌طور فزاینده‌ای زمان‌بر و مستعد خطا شده و پیکربندی نادرست سیاست‌ها، اثربخشی این سیستم‌ها را کاهش داده‌است. محققان، روش‌های کنترل دسترسی پویا را به عنوان راه‌کاری مؤثری برای صدور مجوز در این سیستم‌ها توصیه می‌کنند. از آنجا که منابع تصمیم‌گیری در این روش‌ها، سیاست‌های تعریف شده و سوابق کاربران است، برای کاربران تازه‌وارد محدودیت خاصی در نظر گرفته نمی‌شود و این روش‌ها با مشکل شروع سرد روبرو هستند. در این مقاله برای رفع این محدودیت از مفاهیم اعتماد و I-sharing استفاده‌شده و روش جدیدی برای بهبود چارچوب مجوز خودتطبیق (SAAF) به نام ISAAF ارائه‌شده است. ISAAF چارچوبی برای کنترل خودتطبیق سیستم‌های مجوز با استفاده از مدل مرجع خودمختار MAPE-K است که اعتماد کاربران تازه‌وارد را با استفاده از خصوصیات کاربرانی که با آن‌ها ویژگی‌های مشترک دارند تخمین می‌زند. گروه‌های I-sharing که دربرگیرنده کاربران مشابه هستند، با توجه به نقش و ویژگی‌های هویتی کاربران و با استفاده از خوشه‌بندی K-means تشکیل می‌شوند. بهره‌گیری از مفاهیم اعتماد و I-Sharing و گروه‌بندی کاربران با استفاده از نقش و ویژگی‌های هویتی آن‌ها، برای اولین بار در این مقاله پیشنهاد شده و نتایج تجربی حاکی از آن است که روش پیشنهادی در مقایسه با روش‌های مشابه نتایج بهتری از حیث صحت یافتن کاربران مخرب و کاهش زمان فعالیت آن‌ها در سیستم تولید می‌کند. مزیت دیگر این روش پیاده‌سازی عناصر حلقه MAPE-K و کاربران با استفاده از عامل‌ها است که موجب استقلال و انعطاف‌پذیری بیشتر سیستم می‌شود. در مقایسه با SAAF، ISAAF به‌طور میانگین، زمان یافتن کاربران مخرب را ۵۵ درصد کاهش داده و دقت شناسایی کاربران مخرب را نیز بیش از ۷ درصد بهبود بخشیده است.

واژه‌های کلیدی: چارچوب مجوز خودتطبیق، اعتماد، شروع سرد، حملات خودی، I-Sharing.

۱- مقدمه

تأمین امنیت سیستم‌های پویا و ناهمگن چالش‌برانگیز است زیرا مکانیسم‌های امنیتی ایستا نمی‌توانند برای سناریوهای پویا مناسب باشند و پیش‌بینی همه زمینه‌ها و شرایط سیستم‌ها اغلب امکان‌پذیر نیست. با پیشرفت سیستم‌ها، تعداد و پیچیدگی تهدیدات امنیتی افزایش می‌یابد؛ نمونه‌ای از چنین ریسک‌هایی، سوءاستفاده کاربر از دسترسی مجاز خود برای انجام حملات خودی[۱] است. امنیت خودتطبیق می‌تواند راه‌حلی مناسب برای سیستم‌هایی باشد که اقدامات امنیتی ایستا برای آن‌ها کافی نیست؛ زیرا قادر است به‌طور مستقل و در زمان اجرا سازوکارهای

امنیتی و تنظیمات خود را مطابق با وضعیت و نیازهای فعلی سیستم و محیط آن تطبیق دهند[۱]. برای کنترل دسترسی به منابع و خدمات از مدل‌های کنترل دسترسی استفاده می‌شود. پرکاربردترین مدل‌های کنترل دسترسی، مدل‌های کنترل دسترسی مبتنی بر نقش[۲] (RBAC) [۲] و مدل‌های کنترل دسترسی مبتنی بر ویژگی[۳] (ABAC) [۳] هستند. در سال‌های اخیر برای حفظ امنیت سیستم‌های کامپیوتری از روش‌های خودتطبیق استفاده‌های متعددی شده است درزمینهٔ کنترل دسترسی نیز روش‌های خودتطبیق معدودی ارائه‌شده‌اند که کنترل دسترسی سازگار با ریسک RADac[۴] [۴] و رویکرد SecuriTAS[۵][۵] از آن جمله‌اند. هر دو روش RADac و SecuriTAS، مدل کنترل دسترسی سفارشی و زیرساخت مجوز خود را دارند که خودتطبیقی را در طراحی آن‌ها ترکیب می‌کند، اما نمی‌توان مدل‌های کنترل دسترسی موجود را با این روش‌ها پیکربندی کرد. Bailey و همکاران [۶, ۷] چارچوب مجوز خودتطبیق[۶] (SAAF) را برای کنترل دسترسی مبتنی بر نقش و ویژگی ارائه کرده‌اند. چارچوب مجوز خودتطبیق یک مؤلفه اصلی برای اجرای مدیریت خودتطبیق و یکپارچه‌سازی زیرساخت‌های مجوز دسترسی، مبتنی بر نقش است که در آن از مدل مرجع خودمختار MAPE-K[۷] به‌عنوان راه‌حلی برای شناسایی رفتارهای مخرب و صدور مجوز استفاده شده است. مزیت SAAF نسبت به روش‌های دیگر آن است که توضیح می‌دهد چگونه مدل‌های کنترل دسترسی و زیرساخت‌های مجوز موجود می‌توانند خودتطبیق شده و برای کاهش تهدیدهای داخلی پیکربندی شوند. بااین‌حال SAAF دارای محدودیت‌هایی نیز هست. ازآنجاکه منابع تصمیم‌گیری SAAF سیاست‌های تعریف‌شده و سوابق کاربران است، برای کاربران تازه‌وارد که دارای لیست سوابق نیستند محدودیت خاصی در نظر گرفته نمی‌شود و این کاربران در صورت مخرب بودن تا زمانی که به‌اندازه کافی در سیستم فعالیت نکرده باشند، قابل تشخیص نیستند. درواقع چارچوب مجوز خودتطبیق با مشکل شروع سرد روبرو است.

برای حل مشکل شروع سرد در روش‌های مبتنی بر اعتماد می‌توان از ایده I-sharing بهره برد. پینل و همکاران [۸] مفهوم I-sharing را بیان کردند و نشان دادند که گروهی از افراد که تجربیات ذهنی مشابهی با یکدیگر دارند، به‌احتمال‌زیاد در شرایط معین واکنش-های مشابهی نشان می‌دهند. با توجه به این مفهوم هنگامی‌که یک کاربر جدید تقاضای دسترسی به سیستم را دارد و سابقه‌ای از وی موجود نیست، می‌توان با توجه به ویژگی‌هایش و بر اساس سوابق کاربرانی که ویژگی‌های مشابهی با او دارند بدون هیچ‌گونه تعامل قبلی، مجوز دسترسی مناسب صادر کرد. مفهوم I-sharing و تأثیر آن بر گروه‌های اجتماعی در حوزه روانشناسی موردبررسی قرار گرفته است[۹]. بااین‌حال، کارهای مهندسی کمی این مفهوم را برای افزایش قابلیت انتقال اعتماد در زمینه‌های مشابه به کار گرفته‌اند. روش‌های ارائه شده توسط Gwak و همکاران [۱۰] و Yang و همکاران [۱۱] از I-sharing برای حل مشکل شروع سرد بهره می‌برند. در هر دو کار ذکر شده گروه‌های I-Sharing (گروه‌هایی از کاربران با ویژگی مشابه) تنها با توجه به ویژگی نقش ایجادشده‌اند و سایر ویژگی‌های هویتی کاربر برای سنجش میزان شباهت نادیده گرفته‌شده‌اند.

همان‌طور که گفته شد چارچوب مجوز خودتطبیق نسبت به سایر روش‌های کنترل دسترسی پویا، مؤثرتر عمل می‌کند اما دارای محدودیت‌هایی نیز هست. در این مقاله برای بهبود امنیت، پویایی و حل مشکل شروع سرد SAAF روشی ارائه شده که آن را ISAAF[8] می‌نامیم. روش پیشنهادی به دو صورت عملکرد SAAF را بهبود می‌بخشد: ابتدا با تصمیم‌گیری مبتنی بر اعتماد و منطق ذهنی[۱۲] و دوم با استفاده از مفهوم I-sharing [۸] برای رفع مشکل شروع سرد. صدور مجوز خودتطبیق و کنترل دسترسی به‌صورت پویا، در SAAF توسط حلقه MAPE-K انجام می‌شود. روش پیشنهادی با استفاده از مفهوم اعتماد و منطق ذهنی در مؤلفه تحلیل، امنیت و محرمانگی را در طول فرآیند دسترسی به داده، افزایش می‌دهد. به این منظور رفتار کاربران به‌طور مداوم رصد شده و اعتماد سیستم به آن‌ها محاسبه می‌شود. در صورت کاهش اعتماد کاربر به زیر حد آستانه، دسترسی وی به سیستم قطع می‌شود. در ISAAF اعتماد اولیه کاربران تازه‌وارد، از گروه I-Sharing که به آن تعلق دارند محاسبه می‌شود. بهره‌گیری از مفهوم I-Sharing و گروه‌بندی کاربران با استفاده از نقش و ویژگی‌های هویتی آن‌ها، برای اولین بار در این مقاله استفاده شده است. ازآنجاکه گروه‌بندی کاربران بایستی بر اساس ویژگی‌های متعدد صورت پذیرد، از خوشه‌بندی K-means برای دسته‌بندی کاربران استفاده شده است. علاوه بر این، پیاده‌سازی مبتنی بر عامل ISAAF موجب استقلال و انعطاف‌پذیری بیشتر آن می‌شود [۱۳]. وجه تمایز روش پیشنهادی نسبت به روش‌های کنترل دسترسی موجود، عبارت است از افزودن مفهوم اعتماد و محاسبه آن با استفاده از منطق ذهنی به چارچوب مجوز خودتطبیق (SAAF) و تعیین اعتماد اولیه کاربران تازه‌وارد با بهره‌گیری از مفهوم I-Sharing و گروه‌بندی کاربران با استفاده از نقش و ویژگی‌های هویتی متعدد آن‌ها. استفاده از مفهوم I-Sharing تنها در روش‌های ارائه‌شده توسط Gwak و همکاران [۱۰] و Yang و

همکاران [۱۱] برای حل مشکل شروع سرد استفاده شده است اما در هر دو مورد، گروه‌های I-Sharing تنها با توجه به نقش کاربران ایجاد شده‌اند و سایر ویژگی‌های هویتی آن‌ها نادیده گرفته شده است. این در حالی است که در روش پیشنهادی گروه‌های I-Sharing با توجه به نقش و ویژگی‌های متعدد هویتی ایجاد شده‌اند و به علت تعدد ویژگی‌ها برای ایجاد گروه‌ها از خوشه‌بندی K-means استفاده شده است. بر اساس نتایج تجربی به‌دست‌آمده، روش پیشنهادی در مقایسه با روش‌های مشابه نتایج بهتری از حیث صحت یافتن کاربران مخرب و کاهش زمان فعالیت آن‌ها در سیستم تولید می‌کند.

ادامه این مقاله به شرح زیر است: ابتدا در بخش دوم، به برخی از کارهای انجام شده در این حوزه اشاره شده است. در بخش سوم مفاهیم مرتبط مختصراً شرح داده‌شده‌اند. در بخش چهارم روش پیشنهادی برای بهبود چارچوب مجوز خودتطبیق (ISAAF) ارائه شده است. بخش پنجم به جزئیات پیاده‌سازی، نتایج تجربی و بحث در مورد نتایج پرداخته و درنهایت، نتیجه‌گیری در بخش ششم آمده است.

۲- کارهای مرتبط

کنترل دسترسی و اعتماد از حوزه‌های مهم و گسترده محیط‌های دیجیتال هستند. توسعه دستی این سیستم‌ها، زمان‌بر و مستعد خطا است. علاوه بر این، پیکربندی نادرست سیاست‌ها، اثربخشی سیستم‌های کنترل دسترسی را کاهش می‌دهد. استفاده از روش‌های کنترل دسترسی پویا و خودتطبیق می‌تواند راه‌کار مؤثری برای افزایش امنیت این سیستم‌ها باشد. در این بخش ابتدا به معرفی رویکردهای خودحفاظتی از طریق کنترل دسترسی پرداخته و در ادامه روش‌های ارائه شده برای حل مشکل شروع سرد در این حوزه را به‌طور مختصر بیان می‌کنیم.

۲-۱- خودحفاظتی از طریق کنترل دسترسی

سیستم‌های خودحفاظتی[۹] نوعی از سیستم‌های خودتطبیق با هدف کاهش رفتارهای مخرب هستند که از مدل‌های کنترل دسترسی بهره می‌برند. در ادامه، به معدود آثاری می‌پردازیم که درزمینه‌ی کاهش حملات خودی، از خودحفاظتی بهره برده‌اند. یکی از این روش‌ها، مقابله با تهدیدهای خودی، از طریق کنترل دسترسی سازگار با ریسک RADac[۱۰] [۴] است. کنترل دسترسی سازگار با ریسک، به دنبال تشخیص ریسک‌ها برای محافظت از منابع (در زمان اجرا)، با استفاده از عوامل داخلی و خارجی است. بر اساس ریسک تشخیص داده‌شده، سطح دسترسی برای کاربر به‌طور پویا تغییر می‌کند. در این رویکرد درک یک سیستم از محیط خود منجر به تغییر و انطباق در نحوه تصمیم‌گیری برای دسترسی می‌شود. این رویکرد، بر اساس حقوق دسترسی کاربر و اعتماد (که در آن ارزش اعتماد از فعالیت کاربر محاسبه می‌شود) اداره می‌شود و خط‌مشی‌های کنترل دسترسی با آستانه‌های اعتماد تنظیم می‌شوند.

یکی دیگر از رویکردهای خودحفاظتی از طریق کنترل دسترسی، SecuriTAS[۱۱] [۵] است. هدف SecuriTAS فعال کردن تصمیمات پویا در اعطای دسترسی، بر اساس وضعیت درک شده از سیستم و محیط است. این روش، شبیه رویکردهای کنترل دسترسی پویا، مانند RADac [۴] است، زیرا مفهومی از ریسک برای منابع تعریف می‌کند به‌طوری‌که تغییر در تهدیدها منجر به تغییر در تصمیمات کنترل دسترسی می‌شود. SecuriTAS، RADac را با گنجاندن مفهوم سودمندی ارتقا می‌دهد که به‌موجب آن با توجه به وضعیت درک شده از سیستم، مجموعه‌ای بهینه از کنترل‌های امنیتی استفاده می‌شوند. این امر از طریق استفاده از یک کنترل‌کننده MAPE-K محقق می‌شود که مجموعه‌ای از مدل‌ها را در زمان اجرا تجزیه‌وتحلیل و بروز می‌کند. روش SecuriTAS با به‌کارگیری رویکرد خودتطبیق برای کنترل دسترسی، در کاهش حملات خودی، مؤثر عمل می‌کند. این یک مزیت اضافی در مقایسه با روش‌های کنترل دسترسی ایستا (به‌عنوان‌مثال، RBAC) است. هر دو روش RADac و SecuriTAS، مدل کنترل دسترسی سفارشی و زیرساخت مجوز خود را دارند که خودتطبیقی را در طراحی آن‌ها ترکیب می‌کند، اما نمی‌توان مدل‌های کنترل دسترسی موجود را با این روش‌ها پیکربندی کرد.

Bailey و همکاران [۶, ۱۳] چارچوب مجوز خودتطبیق (SAAF) را برای شناسایی و پاسخگویی به آسیب‌پذیری‌هایی که مشابه تهدیدات خودی هستند، پیشنهاد کردند. معماری SAAF از توابع مدل MAPE-K تشکیل شده است و هدف آن نظارت بر استفاده از زیرساخت مجوز، استدلال در مورد رفتار کاربران در مورد درخواست‌های مجوز و انطباق مناسب زیرساخت است. چارچوب SAAF واکنشی است، به این معنی که اگر یک رفتار غیرعادی شناسایی شود، سیستم به‌طور مستقل تصمیم می‌گیرد که آیا زیرساخت مجوز باید تغییر کند یا خیر. از طریق تغییر ویژگی‌ها، مجوزهای دسترسی را می‌توان کاهش یا افزایش داد. زیرساخت از یک مدل سیاست استفاده می‌کند که حاوی قوانین رفتاری است و می‌تواند امکان تشخیص استفاده غیرعادی از مجوز را فراهم کند. قوانین رفتاری دارای توابع هزینه هستند که نشان‌دهنده تأثیر آن رفتار بر سیستم در صورت شکسته شدن یک قانون است.

زیرساخت همچنین به آمار استفاده بستگی دارد که به سیستم اجازه می‌دهد تا در مورد نقش‌ها، ویژگی‌ها، موضوعات و مجوزها نتیجه‌گیری کند [۱۴]. مزیت اصلی SAAF نسبت به SecuriTAS و RADac این است که SAAF چارچوبی است که توضیح می‌دهد چگونه مدل‌های کنترل دسترسی و زیرساخت‌های مجوز موجود می‌توانند خودتطبیق شده و برای کاهش تهدیدهای داخلی پیکربندی شوند.

با این‌که رویکردها ذکر شده موجب استحکام زیرساخت مجوز در کاهش حملات خودی می‌شوند و از تداوم حملات، به‌صورت خودتطبیق جلوگیری می‌کند اما با مشکل شروع سرد روبرو هستند.

۲-۲- مشکل شروع سرد

همان‌طور که گفته شد، منابع تصمیم‌گیری رویکردهای خودحفاظتی، عبارت‌اند از وضعیت درک شده از سیستم و محیط، سیاست‌های تعریف شده و سوابق قبلی کاربران، لذا برای کاربران تازه‌واردی که دارای لیست سوابق نیستند محدودیت خاصی در نظر گفته نمی‌شود و این کاربران در صورت مخرب بودن تا زمانی که به‌اندازه کافی در سیستم فعالیت نکرده‌اند و سوابق کافی از آن‌ها ثبت نشده است، قابل تشخیص نیستند. درواقع رویکردهایی که مبتنی بر اعتماد هستند به‌نوعی با مشکل شروع سرد روبرو هستند. برخی روش‌های مدیریت اعتماد با تخصیص یک مقدار اعتماد اولیه اختیاری به این مشکل می‌پردازند [۱۵, ۱۶]، درحالی‌که برخی روش‌های دیگر آن را نادیده گرفته‌اند [۲۲-۱۷]. اختصاص مقدار اعتماد ثابت به کاربران و دستگاه‌های تازه‌وارد می‌تواند عملکرد کل سیستم را مختل کند، هنگامی‌که یک مقدار اعتماد بالا به یک کاربر یا دستگاه مخرب داده شود، منجر به سیاست‌های ناعادلانه و کاهش امنیت سیستم می‌شود، درحالی‌که اگر اعتماد کاربر یا دستگاه‌های درستکار کم در نظر گرفته شود باعث عملکرد ضعیف سیستم می‌شود. برخی محققان از شهرت و توصیه‌های سایر کاربران برای پیش‌بینی اعتماد اولیه بهره می‌برند [۲۵-۲۳] بااین‌حال، یکسان نبودن زمینه‌ها، ممکن است باعث تخمین اعتماد نادرست شود.

برخی از محققان از شباهت نقش کاربران برای محاسبه اعتماد اولیه استفاده کرده‌اند و به این منظور کاربران را گروه‌بندی کرده و میانگین اعتماد هر گروه را به‌عنوان اعتماد اولیه کاربر تازه‌وارد در نظر می‌گیرند. HOU و همکاران [۲۶]، مکانیسم کنترل دسترسی ریزدانه (FGAC[12]) را برای اطمینان از امنیت داده‌های محاسبات لبه موبایل پیشنهاد کردند. در FGAC، بر اساس تئوری متاگراف، روشی ریزدانه برای گروه‌بندی کاربران ارائه شده است. این طرح با فنون کنترل دسترسی مبتنی بر نقش ترکیب شده تا بر اساس اعتبار گروه‌های کاربری، نقش‌هایی را به کاربران اختصاص دهد. سپس، بر اساس تطبیق نقش کاربر، سیستم احراز هویت تأیید می‌کند که آیا کاربر برای انجام عملیات دسترسی خاص، مجاز است یا خیر. روش FGAC می‌تواند به‌طور مؤثری کاربران مخرب را شناسایی کرده و تنظیمات امنیتی گروه‌های کاربری را انجام دهد.

Gwak و همکاران [۱۰] یک سیستم کنترل دسترسی مبتنی بر اعتماد و نقش برای اینترنت اشیا (TARAS) پیشنهاد می‌کنند که بر اساس برآورد اعتماد پویا، مجوز ورودِ خودتطبیق برای کاربران فراهم می‌کند. در این روش برای ارزیابی اعتماد از سابقه‌ی تعاملات قبلی کاربران و برای تعیین اعتماد اولیه از مفهوم I-Sharing استفاده شده است. در TARAS گروه‌های I-Sharing تنها بر اساس ویژگی نقش کاربران تشکیل شده‌اند و سایر ویژگی‌ها در نظر گرفته نشده‌اند.

همان‌طور که در بخش ۲-۱ بیان شد SAAF، فارغ از مشکل شروع سرد، کارایی مطلوبی دارد. مفهوم I-Sharing از این منطق پیروی می‌کند که افراد با ویژگی‌های مشابه احتمال بیشتری دارد که به شیوه‌ای مشابه رفتار کنند. لذا در این مقاله برای رفع مشکل شروع سردِ SAAF، از مفهوم I-Sharing استفاده شده و اعتماد اولیه کاربران با استفاده از ویژگی نقش و سایر ویژگی‌های هویتی آن‌ها، محاسبه شده است. درنتیجه با بهره‌گیری از مفهوم اعتماد و تخمین اعتماد اولیه کاربران تازه‌وارد، کارایی SAAF بهبود یافته است.

۳- مرور مفاهیم استفاده شده

در این بخش، روش دسترسی ایستا و پویا، چارچوب مجوز خودتطبیق و I-Sharing، به‌طور مختصر تعریف شده‌اند.

۳-۱- کنترل دسترسی ایستا و پویا

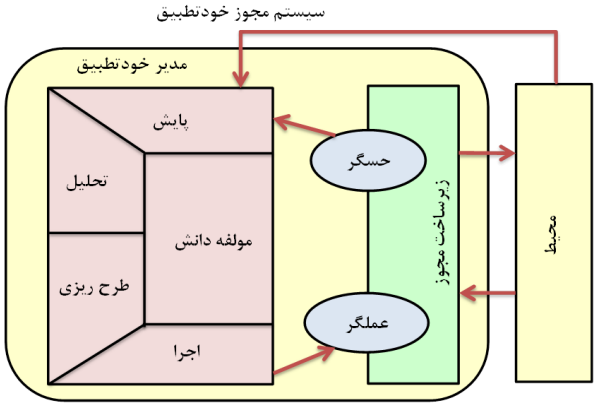
این بخش به تمایز بین رویکردهای سنتی (ایستا) و رویکردهای جدیدتر (پویا) برای کنترل دسترسی پرداخته است. در رویکردهای ایستا، مجوزهای دسترسی کاربران با استفاده از مجموعه‌ای از کنترل‌های امنیتی ثابت، صادر می‌شوند و هیچ زمینه اضافی مانند دسترسی‌های گذشته کاربر، موقعیت مکانی، زمان یا سایر عوامل در نظر گرفته نمی‌شوند. به‌عنوان مثالی از این نوع کنترل دسترسی می‌توان به RBAC اشاره کرد. رویکردهای کنترل دسترسی پویا به سازمان‌ها اجازه می‌دهد تا در پاسخ به ریسک‌ها،

تهدیدها و وضعیت‌های محیطی، کنترل دقیق‌تری را روی دسترسی تعریف کنند. کنترل دسترسی پویا با ایستا ازاین‌جهت متفاوت است که می‌تواند از کنترل‌های امنیتی مختلفی که مربوط به تغییرات در وضعیت محیط یا منابع محافظت‌شده و فعالیت کاربران است، استفاده کند. به‌این‌ترتیب، یک سیاست مجوز ممکن است شامل مجموعه متنوعی از قوانین کنترل دسترسی باشد تا سناریوهای مختلفی را در خود جای دهد.[۲۷]. هدف کنترل دسترسی پویا کاهش مداخلات انسانی، پاسخگویی بیشتر به حملات و مقرون به‌صرفه‌تر شدن است. چندین تکنیک پیشنهاد شده عبارت‌اند از استفاده از اعطای دسترسی بر اساس ویژگی‌های منابع[۱۳] [۲۸]، ویژگی‌های زمانی[۱۴] [۲۹]، ریسک [۴] و اعتماد[۱۵] [۳۰, ۳۱]. علاوه بر این، ABAC [۳] را می‌توان به‌عنوان یک مدل کنترل دسترسی پویا با توجه به توانایی آن در تعریف مجوزهایی که می‌تواند برای بسیاری از وضعیت‌های سیستم معتبر باشد، در نظر گرفت.

۳-۲- زیرساخت مجوز خودتطبیق

با هدف کاهش مداخله انسانی، خودتطبیقی را می‌توان در زیرساخت‌های مجوز موجود طراحی و ایجاد کرد تا آن‌ها را قادر سازد در زمان اجرا، تعریف سیاست‌های مجوز و فرآیند کنترل دسترسی را مدیریت کنند. به‌طور خاص، در زیرساخت‌های مجوز خودتطبیق تمرکز بر این است که چگونه خودتطبیقی می‌تواند با زیرساخت‌های مجوز ادغام شود تا آن‌ها را در برابر تهدیدات داخلی محافظت کنند. خودتطبیقی یک سیستم را قادر می‌سازد تا خود را در پاسخ به تغییراتی که ممکن است بر خودش یا محیط تأثیر بگذارد، تنظیم کند. به‌طورکلی سیستم‌های خودتطبیق، سیستم‌هایی هستند که می‌توانند رفتار و/یا ساختار خود را در پاسخ به تغییراتی که برای خود سیستم، محیط آن یا حتی اهداف آن رخ می‌دهد، اصلاح کنند [۳۲]. چندین مدل مرجع برای سیستم‌های خودتطبیق وجود دارد [۳۳-۳۵]. مدل مرجع MAPE-K از رایج‌ترین مدل‌های حلقه کنترل بازخورد و شامل مؤلفه‌های پایش، تجزیه‌وتحلیل، برنامه‌ریزی، اجرا و پایگاه دانش است [۳۳]. در این مدل، حلقه کنترل بازخورد اصلی، پایش را از طریق حسگر و اجرای تطبیق را از طریق عملگر روی سیستم هدف پیاده‌سازی می‌کند. مرحله پایش امکان به دست آوردن وضعیت سیستم هدف و محیط آن را فراهم می‌کند. مرحله تجزیه‌وتحلیل وضعیت سیستم هدف و محیط آن را تحلیل کرده تا تصمیم بگیرد که آیا تطبیق باید انجام شود یا خیر و در صورت نیاز به تطبیق، اقدامات و راه‌حل‌های مناسب را تعیین می‌کند. مرحله برنامه‌ریزی، از میان راه‌حل‌ها، آن‌هایی را که مناسب‌ترین هستند، انتخاب می‌کند و طرح‌هایی را تولید می‌کند که مسیر عمل انتخابی را محقق می‌سازد. مرحله اجرا، طرح‌ها را اجرایی می‌کند. درنهایت، پایگاه دانش، هرگونه اطلاعات مربوط به وضعیت درک شده سیستم و محیط را که امکان تطبیق را فراهم می‌کنند، جمع‌آوری و به‌روز می‌کند.

با استفاده از مدل مرجع MAPE-K، یک ساختار زیرساخت مجوز را به‌عنوان سیستم هدف و بقیه، ازجمله کاربران و منابع محافظت‌شده را به‌عنوان محیط می‌بینیم. مدل MAPE-K نقش یک کنترل‌کننده برای نظارت بر سیستم هدف و محیطی که در آن تغییرات در زیرساخت مجوز ایجاد می‌شوند را بر عهده دارد. با در نظر گرفتن این موضوع، خودتطبیقی می‌تواند رویکردهای سنتی را برای کنترل دسترسی گسترش دهد، چنین رویکردهایی می‌توانند به حالت‌های برنامه‌ریزی نشده پاسخ دهند، نیازهای کاربر را تغییر دهند و محرمانگی، یکپارچگی و در دسترس بودن منابع را تضمین کنند. مدل سیستم مجوز خودتطبیق در شکل ۱ نشان داده شده است. بر اساس موارد فوق، مجوز خودتطبیق، به تطبیق مشخصات دسترسی به منابع، در زمان اجرا اشاره دارد. کنترل دسترسی خودتطبیق، به اجرای مجوز از طریق کنترل دسترسی به یک منبع اطلاق شده و زیرساخت مجوز خودتطبیق به انطباق مجموعه سیاست‌های مجوز و اجرای آن‌ها در زمان اجرا گفته می‌شود [۲۷].



شکل ۱: معماری سیستم مجوز خودتطبیق[۶].

۳-۳- چارچوب مجوز خودتطبیق (SAAF)

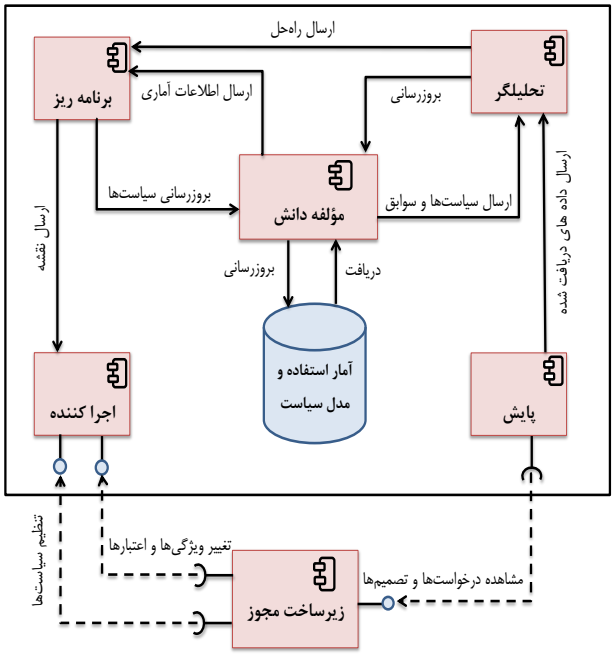
Bailey و همکاران [۶, ۷, ۱۳] چارچوب مجوز خودتطبیق را برای سیستم‌های RBAC / ABAC ارائه کرده‌اند. معماری SAAF که در شکل ۲ نشان داده‌شده است، مدل مرجع MAPE-K را مجسم می‌کند. پایش، یک مؤلفه ساده است که از طریق آن زیرساخت

مجوز مشاهده می‌شود. به‌عنوان‌مثال، درخواست‌های دسترسی و تصمیم مربوط به مجوز را ضبط می‌کند و آن را به تحلیل‌گر می‌فرستد. هدف تحلیل‌گر، پردازش داده‌های پایش شده است؛ برای تشخیص اینکه آیا رفتار غیرطبیعی رخداده است یا خیر. برای این کار، به مدل سیاست و سوابق کاربر که از پایگاه دانش حاصل‌شده است، تکیه می‌کند. تحلیل‌گر پایگاه دانش را با داده‌های تحلیل شده به‌روز می‌کند (تا برای تجزیه‌وتحلیل در آینده مورد استفاده قرار گیرند) و مجموعه‌ای از راه‌حل‌هایی که ممکن است باعث جلوگیری یا پذیرش رفتار غیرعادی و مخرب شوند، برای برنامه‌ریز فراهم می‌کند. این کار به‌صورت اصلاح قوانین یا اضافه یا حذف کردن امتیازات یک کاربر انجام می‌شود. نقش برنامه‌ریز انتخاب مقرون به‌صرفه‌ترین راه‌حل از مجموعه راه‌حل‌های ارائه‌شده توسط تحلیل‌گر است. سپس راه‌حل انتخاب شده برای به‌روزرسانی مدل سیاست، به پایگاه دانش ارسال می‌شود و به طرحی تبدیل می‌شود که برای اجراکننده فرستاده می‌شود. اجراکننده زیرساخت مجوز را مطابق با طرح، تطبیق می‌دهد، درنتیجه، ویژگی‌های کاربر، اعتبارنامه و مدیریت سیاست‌های مجوز اصلاح می‌شوند. موتور تصمیم‌گیری SAAF ترکیبی از تحلیل‌گر و برنامه‌ریز است. آن‌ها چهار فعالیت اصلی را انجام می‌دهند: تحریک تطبیق، تحلیل، انتخاب راه‌حل و تولید برنامه. محرک تطبیق وظیفه تشخیص رفتار مخرب و شروع عملیات تطبیق را به عهده دارد و تحلیل راه‌حل‌های ممکن را یافته و به مؤلفه برنامه‌ریز می‌فرستد. محرک تطبیق و تحلیل فعالیت‌های مؤلفه تحلیل‌گر هستند. انتخاب راه‌حل و تولید برنامه که فعالیت‌های مؤلفه برنامه‌ریز می‌باشند نیز به ترتیب بهترین راه‌حل را انتخاب کرده و روش اجرای آن را تعیین می‌کنند. به‌طورکلی هدف موتور تصمیم‌گیری، شناسایی رفتار غیرطبیعی، از نظر سوءاستفاده در دسترسی به منابع و انتخاب یک راه‌حل و تحقق آن از طریق تطبیق، به‌منظور جلوگیری از چنین رفتاری است [۳۶]. فرآیند موتور تصمیم‌گیری در شکل ۳ نشان داده‌شده است.

۴-۳- مفهوم I-sharing

Pinel و همکاران [۸] اصطلاح I-sharing را برای اولین بار بیان کردند گروهی از افراد که تجربیات ذهنی مشابهی با یکدیگر دارند، به‌احتمال‌زیاد در شرایط مشابه واکنش‌های مشابهی بروز می‌دهند. اگر فردی در یک لحظه معین چیزی را تجربه کند، تصور می‌کند که شخصی که تجربه مشابه با وی دارد نیز آن را همان‌طور که او تجربه می‌کند، تجربه خواهد کرد. برای مثال، اگر دو نفر در پاسخ به یک شوخی به‌طور هم‌زمان بخندند، احساس می‌کنند که موقعیت فعلی را به‌طور یکسان تجربه کرده‌اند. اگر آن‌ها مکرراً لحظات مشابهی را با یکدیگر تجربه کنند، خود را شبیه و مرتبط می‌دانند و تمایل دارند رفتار یا افکار دیگری را در خود ببینند. بر اساس این مفهوم، تجربه ذهنی یک کاربر را می‌توان با تجربه دوستان او، (دوستانی که دارای تجربه ذهنی مشترک با او هستند) جایگزین کرد. از این ویژگی می‌توان برای تخمین ارزش اعتماد ذهنی کاربر در موقعیت‌هایی که تجربه نکرده است استفاده کرد. هنگامی‌که کاربر با موقعیتی ناشناخته روبرو می‌شود که قبلاً آن را تجربه نکرده است، با مقایسه تجربیات گذشته دوستانش در موقعیت‌های مشابه، می‌تواند در مورد شرایط، دید نسبی پیدا کرده و تصمیم بگیرد.

این تئوری حاکی از کاربرد بالایی در انتقال اعتماد از یک زمینه به زمینه مشابه دیگر است که در آن یک موجودیت انسانی از ویژگی‌های مشابهی از لحاظ نقش در هر دو زمینه برخوردار است. در این تئوری، به مجموعه افرادی که تجارب یا ویژگی‌های مشابهی دارند، یک گروه I-sharing گفته می‌شود. مفهوم I-sharing و تأثیر آن بر گروه‌های اجتماعی در حوزه روانشناسی مورد بررسی قرارگرفته است[۹]. بااین‌وجود، در حوزه مهندسی کارهای اندکی این مفهوم را برای انتقال قابلیت اعتماد در زمینه‌های مشابه به‌کاربرده‌اند. در [۱۰, ۳۷] دو مدل مدیریت اعتماد، با استفاده از مفهوم I-sharing به‌منظور اعتماد به اشخاص ناشناس (یعنی ارائه‌دهندگان خدمات) در محیط‌های عمومی IoT بر اساس اعتماد اعضای گروه I-sharing ارائه‌شده است.



شکل ۲: معماری SAAF [۶].

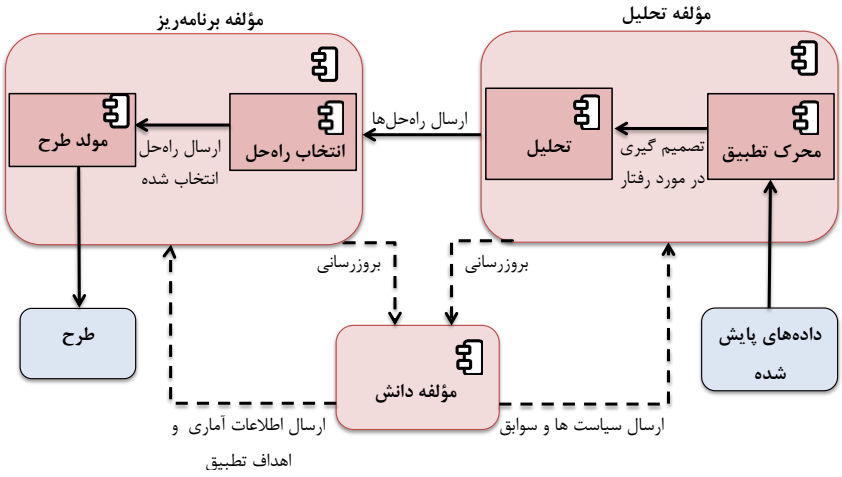
۴- روش ارائه‌شده برای بهبود چارچوب مجوز خودتطبیق

همان‌طور که قبلاً گفته شد چارچوب مجوز خودتطبیق در شکل فعلی محدودیت‌هایی دارد. ازآنجایی‌که منابع تصمیم‌گیری چارچوب مجوز خودتطبیق، سیاست‌های تعریف‌شده و سوابق کاربران هستند، برای کاربران تازه‌وارد که دارای لیست سوابق نیستند محدودیت خاصی در نظر گرفته نمی‌شود و این کاربران در صورت مخرب بودن تا زمانی که به‌اندازه کافی در سیستم فعالیت نکرده‌اند و سوابق کافی از آن‌ها ثبت نشده است، می‌توانند به فعالیت خود ادامه دهند. در این مقاله به دو صورت عملکرد SAAF بهبود یافته است: ابتدا با تصمیم‌گیری مبتنی بر اعتماد و منطق ذهنی در زمان تحلیل و دوم با استفاده از مفهوم I-sharing برای رفع مشکل شروع سرد. در مدل ارائه شده برای بهبود SAAF، مؤلفه مدیر اعتماد که شامل مدیر I-sharing است، به بخش تحلیل‌گر افزوده شده که وظیفه محاسبه اعتماد کاربران، به‌روزرسانی مداوم آن و محاسبه اعتماد اولیه در هنگام ورود کاربران تازه‌وارد را به عهده دارد (شکل ۴). در ادامه روش کار مدیر اعتماد و مدیر I-sharing را شرح می‌دهیم.

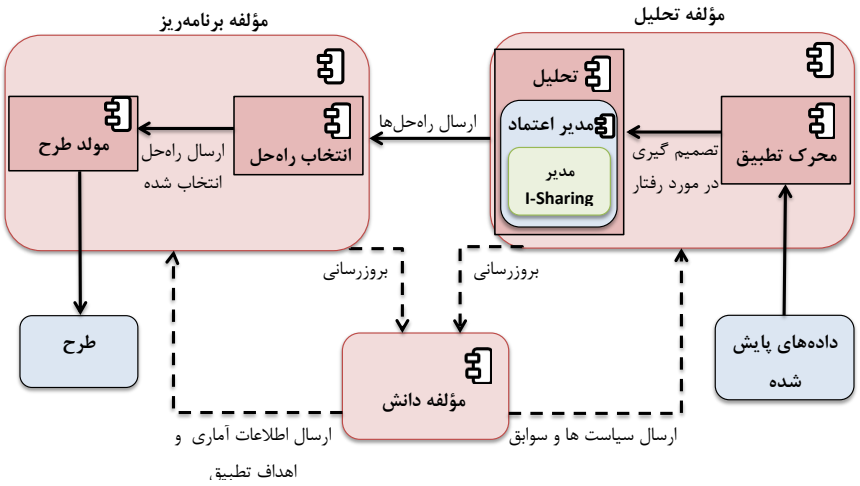
۴-۱- مدیر اعتماد

مؤلفه تحلیل، میزان اعتماد کاربرانی که تقاضای ارتباط با سیستم را دارند تخمین می‌زند. به‌منظور محاسبه اعتماد، مدیر اعتماد از مفهوم منطق ذهنی[۱۶] [۱۲] استفاده می‌کند. منطق ذهنی درجه‌ای از عدم قطعیت را در نظر می‌گیرد که ناشی از عدم وجود شواهد است و معمولاً برای منعکس کردن پدیده‌های طبیعی استفاده می‌شود که با افزایش شواهد راجع به یک موضوع خاص، اعتماد ما به آن افزایش می‌یابد. $Tr_{x,y}$ سطح اعتماد کاربر x است که توسط سیستم y تخمین زده می‌شود و به‌صورت زیر تعریف می‌شود:

$$Tr_{x,y} = b_{x,y} + u_{x,y} * a_{x,y} \quad (۱)$$



شکل ۳: فرایند تطبیق SAAF [۶].



شکل ۴: فرایند تطبیق در روش پیشنهادی ISAAF.

در این رابطه، $b_{x,y}$ بیانگر باور یا همان اعتماد مستقیم y به x است که حاصل تعاملات سیستم و کاربر است، $a_{x,y}$ میزان شهرت x در سیستم y یا همان اعتماد اولیه و $u_{x,y}$ درجه عدم قطعیت به دلیل نداشتن شناخت کافی سیستم از کاربر است. در یک دوجمله‌ای مبتنی بر منطق ذهنی، رابطه زیر برقرار است:

$$b_{x,y} + d_{x,y} + u_{x,y} = 1 \quad (۲)$$

که در آن، $b_{x,y}$ باور یا همان اعتماد مستقیم، $d_{x,y}$ عدم اعتماد و $u_{x,y}$ عدم قطعیت هستند. همه مقادیر تشکیل‌دهنده این رابطه در بازه $[0,1]$ هستند. بر اساس توزیع بتا شرح داده شده در [۱۲]، $b_{x,y}$ با استفاده از رابطه زیر محاسبه می‌شود:

$$b_{x,y} = \frac{r_{x,y}}{r_{x,y} + s_{x,y} + W} \quad (۳)$$

در این رابطه $r_{x,y}$ و $s_{x,y}$ به ترتیب بیانگر تعداد تجربه‌های مثبت و منفی هستند و هر دو مقدار نیز عدد صحیح می‌باشند. W عددی ثابت و بیانگر میزان تأثیر مشاهدات جدید بر اعتماد است که هرچه بیشتر باشد تأثیر مشاهدات جدید کمتر خواهد شد. در این تحقیق، بنا به اهمیت بیشتر مشاهدات جدید نسبت به مشاهدات قبلی، W برابر عدد ثابت ۱ در نظر گرفته شده است. عدم قطعیت $u_{x,y}$ برای ایجاد تعادل بین تعاملات مستقیم و شهرت، در تخمین اعتماد استفاده می‌شود و توسط رابطه زیر محاسبه می‌شود:

$$u_{x,y} = \frac{W}{r_{x,y} + s_{x,y} + W} \quad (۴)$$

توجه کنید که عدم قطعیت $u_{x,y}$ با تجربیات مستقیم، شامل تراکنش‌های مثبت و منفی نسبت عکس دارد. نکته مهم در مورد رابطه (۱) آن است که اگر سیستم y تجربه تعامل قبلی با کاربر x را نداشته باشد، بخش اول رابطه یعنی $b_{x,y}$ برابر صفر می‌شود پس با مشکل شروع سرد روبرو هستیم و تنها اطلاعاتی که از کاربر تازه‌وارد موجود است اطلاعات شهرت آن است و اعتماد فقط با استفاده از شهرت محاسبه می‌شود. با شکل‌گیری تعاملات بین y و x و افزایش تجربیات مستقیم تأثیر $b_{x,y}$ در تعیین اعتماد افزایش می‌یابد درحالی‌که میزان عدم قطعیت و درنتیجه اثرِ بخش دوم رابطه کاهش پیدا می‌کند. این امر کاملاً منطقی است زیرا وقتی اطلاعات مستقیم در موردِ کاربر کافی نباشد بایستی از سایر منابع اطلاعاتی بهره برد اما با افزایش اطلاعات مستقیم تأثیر آن‌ها کاهش می‌یابد.

۴-۲- مدیر I-sharing

در این مقاله تخمین شهرت $a_{x,y}$ با استفاده از مفهوم I-sharing به دست می‌آید. هنگامی‌که کاربر به یک سیستم هدف تقاضای دسترسی می‌دهد، مدیر I-sharing از حساب او ویژگی‌هایش را که شامل تعریف نقش و خصوصیات هویتی می‌شوند، تعیین می‌کند. بر اساس آن‌ها، مدیرI-sharing فهرستی از کاربرانی که قبلاً با سیستم موردنظر تعامل برقرار کرده‌اند، جستجو می‌کند و از میان آن‌ها، افرادی که ویژگی‌های مشابهی با کاربر موردنظر از حیث نقش و خصوصیات هویتی، دارند را مشخص می‌کند. ازآنجاکه مدیر I-sharing در حال حاضر مقادیر اعتماد برای این کاربران را بر اساس تعاملات مستقیم دارد، سیستم می‌تواند از اعتماد آن‌ها استفاده کند تا به‌سرعت میزان اعتماد اولیه یک کاربر جدید را بدون هیچ‌گونه تعامل قبلی تعیین کند. هر چه تعداد کاربرهایی که تعامل قبلی با سیستم داشته‌اند بیشتر باشد، اعتماد کاربر تازه‌وارد با دقت بیشتری پیش‌بینی می‌شود. پس از جمع‌آوری اطلاعاتِ همه کاربرهایی که تعامل قبلی با سیستم داشته‌اند، بایستی آن‌ها را بر اساس ویژگی‌های هویتی و نقش دسته‌بندی کرد. هر کاربر دارای یک لیست هویت است. این لیست شامل اطلاعات مربوط به مشخصات ذاتی و شخصی کاربر است که در هنگام پیوستن او به سیستم باید تکمیل شود. این اطلاعات شامل سن، جنسیت، سطح تحصیلات یا نقش کاربر در سیستم مانند مدیر سیستم، کاربر عادی و ... می‌باشند. اطلاعاتی که در لیست هویت قرار می‌گیرند، ویژگی‌هایی هستند که با توجه به ماهیت سیستم در زمان طراحی تعیین می‌شوند و به‌صورت $Pro = \{Pro_1, Pro_2, \dots, Pro_k\}$ نمایش داده می‌شوند که لیستی از k ویژگی هویت منتخب است. مقادیر لیست هویت طوری نرمال می‌شوند که در بازه‌ی $[0,1]$ قرار بگیرند.

ازآنجاکه ویژگی‌های متعددی در لیست هویت هر کاربر موجود است، در این مقاله، استفاده از یک روش خوشه‌بندی برای گروه-بندی کاربران پیشنهاد شده است. پس از خوشه‌بندی کاربرها، میانگین سطح اعتماد کاربرهای هر خوشه، به‌عنوان سطح اعتماد آن خوشه در نظر گرفته می‌شود. حال کافی است مشخص شود که کاربر تازه‌وارد به کدام خوشه نزدیک‌تر است تا سطح اعتماد آن خوشه به‌عنوان مقدار پیش‌بینی شده برای اعتماد عامل تازه‌وارد در نظر گرفته شود. برای خوشه‌بندی کاربران و تشکیل گروه‌های I-sharing از الگوریتم خوشه‌بندی K -means استفاده شده است [۳۸]. خوشه‌بندی K-means یک روش خوشه‌بندی با یادگیری غیر نظارتی است و به‌طور گسترده در منابع مورد استفاده قرار گرفته است [۳۹, ۴۰]. خوشه‌بندی K-means، کاربران را بر اساس

ویژگی‌های هویتی منتخب ($pro = \{Pro_1, Pro_2, \dots, Pro_k\}$)، به n خوشه که با $\{C_1, C_2, \dots, C_n\}$ نمایش داده می‌شوند، دسته‌بندی می‌کند. نقاط مرکزی خوشه‌ها نیز با $\{\mu_1, \mu_2, \dots, \mu_n\}$ نشان داده می‌شوند. سطح اعتماد هر خوشه با استفاده از رابطه زیر محاسبه می‌شود:

$$Tr_{C_i} = \frac{\sum_{x \in C_i} Tr_x}{m_i} \quad (۵)$$

در این رابطه m_i تعداد کاربران موجود در خوشه C_i و $\sum_{x \in C_i} Tr_x$ مجموع مقادیر اعتماد همه کاربران موجود در خوشه C_i است. پس از خوشه‌بندی، فاصله اقلیدسی میانِ ویژگی‌های نمایه کاربر تازه‌وارد و نقاط مرکزی خوشه‌ها محاسبه شده و با استفاده از رابطه زیر، خوشه‌ای که مرکزش کمترین فاصله با کاربر تازه‌وارد را دارد به‌عنوان گروه I-sharing آن کاربر انتخاب می‌شود.

$$C_i = \underset{i}{\operatorname{argmin}}\{dis(pro, \mu_i)\} \quad (۶)$$

در این رابطه C_i خوشه‌ای است که کاربر به آن تعلق می‌گیرد و $dis(pro, \mu_i)$ فاصله اقلیدسی بین pro و μ_i را با استفاده از رابطه زیر محاسبه می‌کند:

$$dis(pro, \mu_i) = \sqrt{\sum_{j=1}^{k} \left(pro_j - \mu_{ij}\right)^2} \quad (۷)$$

در رابطه بالا k تعداد ویژگی‌ها را نشان می‌دهد. نهایتاً اعتمادِ خوشه‌ای که کمترین فاصله با کاربر را دارد، یعنی C_i به‌عنوان شهرت کاربر تازه‌وارد ثبت می‌شود.

$$a_{x,y} = Tr_{C_i} \quad (۸)$$

و با قرار گرفتن در رابطه (۱) سطح اعتماد هر کاربر تعیین می‌شود.

۵- نتایج تجربی

این بخش به توصیف سناریو، سنجش عملکرد روش پیشنهادی و مقایسه کارایی آن با SAAF و چند روش مشابه می‌پردازد.

۵-۱- توصیف سناریو

سناریو در نظر گرفته شده برای پیاده‌سازی و سنجش عملکرد ISAAF، سیستم مجوز یک کتابخانه است. در کتابخانه سه نقش مدیر، کارمند و عضو تعریف شده‌اند. کاربر با نقش عضو، امکان جستجو و رزرو کتاب را دارد. کاربر نقش کارمند، امکان حذف، اضافه و جستجوی کتاب‌ها و اعضا را دارد و کاربر نقش مدیر، امکان حذف، اضافه و جستجوی کتاب‌ها، اعضا و کارمندان را دارد. همه کاربرانی که قبلاً توسط سیستم احراز هویت، تائید شده باشند مجاز به ورود به سیستم می‌باشند. روش کار سیستم احراز هویت در حوزه این تحقیق نیست. این کاربران ممکن است هک شوند یا به دلایل مختلف مرتکب رفتار بدخواهانه شوند، مثلاً سعی در استخراج حجم زیادی از اطلاعات یا انجام تراکنش‌های زیاد به‌منظور کاهش سطح سرویس‌دهی سیستم را داشته باشند. در این سناریو هدف تشخیص و حذف کاربرانی است که قصد انجام حمله انکار سرویس را دارند، لذا تعداد سرویس‌های درخواستی هر کاربر در واحد زمان، معیار تشخیص کاربران عادی از کاربران مخرب است؛ یعنی کاربری که در زمان معین تعداد درخواست‌هایش از سیستم بیش‌ازحد مشخصی باشد، به‌عنوان کاربر مخرب تشخیص داده شده و از سیستم حذف می‌شوند. در پیاده‌سازی SAAF، کاربران مخرب با توجه به سابقه و تعداد درخواست‌هایشان از سیستم تشخیص داده می‌شوند و کاربران تازه‌وارد تا زمانی که به‌اندازه کافی در سیستم فعالیت نکرده‌اند، معتمد در نظر گرفته می‌شوند. پیاده‌سازی روش پیشنهادی (ISAAF) در دو مرحله انجام می‌شود: آموزش و سنجش. در مرحله آموزش تعداد نسبتاً زیادی از کاربران که درصدی از آن‌ها مخرب هستند با سیستم تعامل می‌کنند و بر اساس نوع رفتارشان سطح اعتماد هر یک مشخص می‌شود. در این مرحله کاربران بر اساس نقش و ویژگی‌های هویتی خود، با استفاده از خوشه‌بندی K-means، به چهار گروه تقسیم می‌شوند. ویژگی‌های هویتی مورد استفاده در این پیاده‌سازی، نقش، سن، جنسیت و سطح تحصیلات کاربر هستند. سطح اعتماد هر گروه از میانگین اعتماد محاسبه شده برای اعضای آن گروه به دست می‌آید. در مرحله سنجش هر کاربر جدیدی که به سیستم وارد می‌شود میزان شهرتش ($a_{x,y}$) را از گروه I-sharing که به آن نزدیک‌تر است، به دست می‌آورد و پس از انجام تعاملات کمی با سیستم، مخرب یا معتمد بودنش تعیین می‌شود.

۵-۲- معیارهای ارزیابی

برای مقایسه و ارزیابی عملکرد، از معیارهای مقدار زمان فعالیت کاربران مخرب در سیستم و میزان دقت سیستم در تشخیص کاربران مخرب استفاده شده است. مقدار زمان فعالیت کاربران مخرب در سیستم برابر با مجموع زمانی است که همه کاربران مخرب قبل از متوقف شدن در سیستم فعالیت می‌کنند.

جدول ۱: ماتریس درهم‌ریختگی

نوع واقعی	نوع پیش‌بینی‌شده	
	معتمد	مخرب
معتمد	TP	FN
مخرب	FP	TN

برای مقایسه دقت، چهار شاخص استاندارد در نظر گرفته می‌شوند که معنای هر شاخص به‌صورت گرافیکی در ماتریس درهم‌ریختگی[۱۷]جدول ۱ نمایش داده شده است [۴۱]. در این جدول TP تعداد کاربران معتمد است که به‌درستی معتمد تشخیص داده شده‌اند، TN تعداد کاربران مخربی است که به‌درستی مخرب تشخیص داده شده‌اند، FP تعداد کاربران مخربی است که به‌اشتباه معتمد تشخیص داده شده‌اند و FN تعداد کاربران معتمد است که به‌اشتباه مخرب تشخیص داده شده‌اند. دقت یک سیستم تخمین، یکی از برجسته‌ترین معیارهای ارزیابی در ادبیات تحقیق است [۴۲] که میزان نزدیکی مقادیر تخمین زده شده به مقادیر واقعی را اندازه می‌گیرد [۴۳]. به‌منظور ارزیابی و مقایسه دقت، معیارهای ارزیابی استاندارد زیر در نظر گرفته می‌شوند:

صحت[۱۸]: نسبت نتایج واقعی پیش‌بینی شده (هم مثبت واقعی و هم منفی واقعی) بر تعداد کل جمعیت پیش‌بینی شده:

$$Accuracy = \frac{TP + TN}{TP + TN + FN + FP} \quad (۹)$$

صحت عینی‌ترین معیار عملکرد است که نسبت مشاهدات پیش‌بینی شده صحیح به کل مشاهدات را نشان می‌دهد. صحت مشخص می‌کند که چند بار سیستم به‌طورکلی درست عمل کرده است. صحت بالا به‌تنهایی دلیل بر برتری یک مدل نیست هرچند، صحت یک معیار عالی است اما فقط زمانی که مجموعه داده‌ها متقارن باشند یعنی مقادیر مثبت کاذب و منفی کاذب تقریباً یکسان باشند؛ بنابراین، برای ارزیابی عملکرد باید پارامترهای دیگر را نیز مدنظر گرفت [۴۴].

دقت[۱۹]: نسبت موارد مثبت پیش‌بینی شده که درواقع مثبت واقعی هستند:

$$Precision = \frac{TP}{TP + FN} \quad (۱۰)$$

دقت، بیان می‌کند که مدل در پیش‌بینی یک دسته خاص چقدر خوب است. دقت بالا به نرخ مثبت کاذب کم مربوط می‌شود و نشان می‌دهد که بسیاری از نمونه‌های مرتبط به‌درستی شناسایی‌شده‌اند، اما اطلاعاتی در مورد نمونه‌های مربوطه که شناسایی نشده‌اند ارائه نمی‌دهد. این اطلاعات توسط معیار حساسیت ارائه می‌شود که بیان می‌کند چند نمونه، در کل مجموعه‌ی نمونه‌های مربوطه، به‌درستی شناسایی شده‌اند. حساسیت[۲۰] نسبت موارد مثبت واقعی است به همه مواردی که مثبت پیش‌بینی می‌شود:

$$Sensitivity = \frac{TP}{TP + FP} \quad (۱۱)$$

حساسیت کم به این معنی است که بسیاری از نمونه‌های مرتبط ناشناس مانده‌اند.

معیار اِف[۲۱]: ترکیبی از معیارهای حساسیت و دقت است و بیانگر هماهنگی آن دو است، یعنی اگر یکی کم و دیگری زیاد شود معیار اف کاهش می‌یابد. این معیار طبق [۴۵] به‌صورت زیر تعریف می‌شود:

$$F - Measure = \frac{2.Precision.Sensitivity}{Precision + Sensitivity} \quad (۱۲)$$

ضریب همبستگی متیو[۲۲] (MCC) [۴۶]: همبستگی بین نوع پیش‌بینی شده و نوع واقعی عامل‌ها را تخمین می‌زند و به‌صورت زیر تعریف می‌شود:

$$MCC = \frac{TP \cdot TN - FP \cdot FN}{\sqrt{(TP + FN)(TP + FP)(TN + FP)(TN + FN)}} \quad (۱۳)$$

معیار اِف و ضریب همبستگی متیو سعی می‌کنند کیفیت یک پیش‌بینی را با ترکیب سایر معیارها در یک مقدار واحد بیان کنند. علاوه بر این، ضریب همبستگی متیو نسخه بی‌طرفانه معیار اِف در نظر گرفته می‌شود، زیرا از هر چهار عنصر ماتریس درهم‌ریختگی استفاده می‌کند [۴۴]. مقدار ضریب همبستگی متیو نزدیک به یک، به این معنی است که پیش‌بینی دقیق‌تر است. مقدار نزدیک به صفر به این معنی است که پیش‌بینی بهتر از حدس تصادفی نیست و مقدار نزدیک به -1 به این معنی است که پیش‌بینی به‌شدت با واقعیت متناقض است.

۵-۳- نتایج شبیه‌سازی و بحث

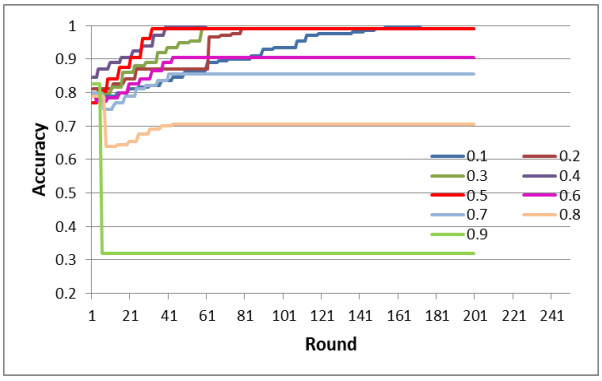
در این سیستم کاربران و عناصر حلقه MAPE-K به‌طور مستقل و موازی عمل می‌کنند، ازاین‌رو این سیستم می‌تواند به‌صورت یک سیستم چندعاملی در نظر گرفته شود. پیاده‌سازی‌ها با استفاده از JADE و در محیط eclipse انجام شده‌اند. همه کاربران و عناصر حلقه MAPE-K به‌صورت عامل‌های مستقل پیاده‌سازی شده‌اند.

هر یک از مؤلفه‌های حلقه MAPE-K وظایف خود را هر ۳۰ ثانیه یک‌بار تکرار می‌کنند و در پایان هر ۳۰ ثانیه مقادیر TP، TN، FP و FN برای انجام ارزیابی‌های بعدی، ذخیره می‌شوند. مرحله آموزش با ۵۰۰ کاربر که ۲۰٪ آن‌ها مخرب هستند انجام می‌شود. کاربران در سیستم شروع به فعالیت کرده و تجربیات سیستم از رفتار آن‌ها ثبت می‌شود. اگر تعداد درخواست‌های یک کاربر در هر دقیقه بیشتر از ۳، در هر پنج دقیقه بیشتر از ۱۰ و در هر ۱۰ دقیقه بیشتر از ۳۰ باشد، آن درخواست یک تجربه منفی ($s_{x,y}$) و در غیر این صورت یک تجربه مثبت ($r_{x,y}$) خواهد بود. پس از ۲۰۰ دور (که هر دور ۳۰ ثانیه به طول می‌انجامد)، سطح اعتماد سیستم به هر کاربر تعیین می‌شود. سپس مجموعه داده‌ای شامل ویژگی‌های هویتی، نقش و میزان اعتماد محاسبه شده برای هر کاربر، ایجاد شده و به الگوریتم K-means داده می‌شود تا گروه‌های کاربری را با توجه به سطوح اعتماد، ایجاد نماید. این مجموعه داده شامل ۵۰۰ سطر به ازای ۵۰۰ کاربر است. برای پیاده‌سازی الگوریتم K -means، تعداد خوشه‌ها برابر چهار در نظر گرفته شده و چهار گروه I-sharing، با سطوح اعتماد مختلف ایجاد شده و میانگین اعتماد اعضای هر گروه به‌عنوان سطح اعتماد آن گروه تعیین می‌گردد.

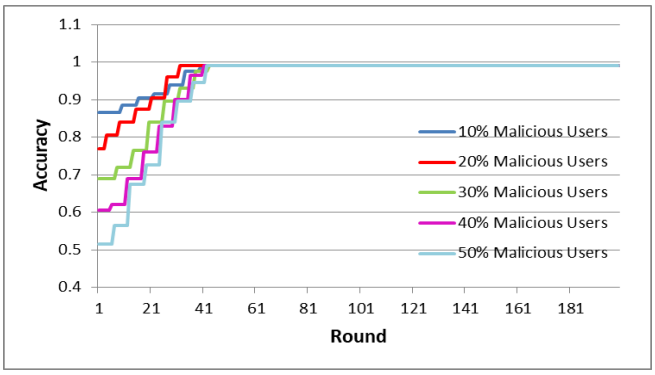
در مرحله سنجش ۲۰۰ کاربر با احتمال مخرب بودن ۲۰٪ به سیستم وارد شده و کاربران مخرب توسط ISAAF تشخیص داده شده و حذف می‌شوند. تشخیص و حذف کاربران مخرب توسط SAAF نیز با ۲۰۰ کاربر با احتمال مخرب بودن ۲۰٪ در ۲۰۰ دور انجام می‌شود و نتایج با روش ارائه شده مقایسه می‌شوند. با توجه به ایده اصلی این مقاله که افزایش کارایی SAAF، با تعیین اعتماد اولیه کاربران تازه‌وارد است، مقایسه برای کاربران، تازه‌وارد انجام شده است.

در پیاده‌سازی ISAAF اگر میزان اعتماد سیستم به کاربر ($Tr_{x,y}$) کمتر از حد آستانه ۰/۵ باشد کاربر مخرب تشخیص داده شده و از سیستم حذف می‌شود. برای یافتن این حد آستانه پیاده‌سازی با همه اعداد بازه صفر تا یک با گام‌های ۰/۱ انجام شده و نتایج به دست آمده در شکل ۵ نمایش داده شده‌اند. همان‌طور که در شکل مشخص است، اگر حد آستانه بیشتر از ۰/۵ باشد، میزان صحت در هیچ یک از موارد به مقدار بیشینه (۰/۹۹) نزدیک نمی‌شود، این امر به دلیل افزایش FN با افزایش حد آستانه است، یعنی تعداد کاربران معتمدی که اشتباهاً مخرب تشخیص داده‌شده‌اند، باعث کم شدن صحت می‌شوند. از طرفی اگر حد آستانه کمتر از ۰/۵ باشد در همه موارد صحت بیشینه به دست می‌آید اما تعداد دورهای بیشتری برای یافتن کاربران مخرب لازم است. پس در این پیاده‌سازی، بهینه‌ترین مقدار برای حد آستانه عدد ۰/۵ است که منتج به بیشترین مقدار صحت، در کمترین زمان می‌شود. در پیاده‌سازی ISAAF احتمال مخرب بودن کاربران ۲۰٪ فرض شده است اما این سیستم در برابر تعداد بیشتر کاربران مخرب نیز مقاوم است و قادر به تشخیص و حذف آن‌ها در زمان تقریباً یکسانی است. برای روشن‌تر شدن این مطلب ISAAF با درصدهای متفاوت کاربران مخرب تست شده است. شکل ۶ نتایج پیاده‌سازی با ۱۰، ۲۰، ۳۰، ۴۰ و ۵۰ درصد از کاربران مخرب را نمایش می‌دهد. با افزایش تعداد کاربران مخرب میزان صحت اولیه سیستم از مقدار کمتری شروع می‌شود اما در تعداد دورهای تقریباً یکسانی همه کاربران مخرب غیرفعال شده و صحت به میزان بیشینه می‌رسد. پس می‌توان نتیجه گرفت که ISAAF در برابر تعداد زیاد کاربران مخرب نیز مقاوم است.

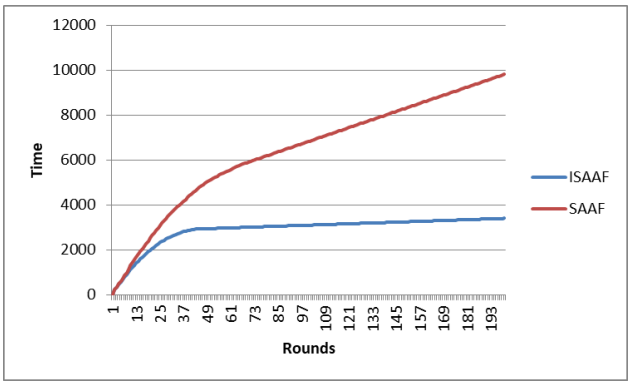
مجموع زمان فعالیت کاربران مخرب در سیستم در هر دو روش SAAF و ISAAF در شکل ۷-الف نمایش داده شده است. با استفاده از ISAAF در دور ۴۴، بیشینه صحت به دست می‌آید و پس از آن زمان حضور کاربران مخرب به‌صورت ثابت رشد می‌کند؛ اما اگر از SAAF برای شناسایی کاربران مخرب استفاده شود بیشینه صحت در دور ۱۰۲ به دست می‌آید و به علت صحت کمترِ SAAF، زمان فعالیت کاربران مخرب در سیستم بیشتر است و با شتاب بیشتری افزایش می‌یابد. به‌طور میانگین ISAAF توانسته است زمان لازم برای شناسایی کاربران مخرب را بیش از ۵۵ درصد کاهش دهد. شکل ۷-ب میزان صحت دو روش را با استفاده از رابطه (۵) نمایش می‌دهد. در هر دو روش کاربران مخرب با درصد بالایی تشخیص داده شده‌اند اما میزان صحت ISAAF در تشخیص کاربران مخرب بالاتر است. علاوه بر این، همان‌طور که در شکل مشخص است با استفاده از روش ISAAF صحت در تعداد دورهای کمتری به مقدار بیشینه می‌رسد. افزایش صحت در شناسایی کاربران مخرب، در ISAAF نسبت به SAAF به‌طور میانگین بیش از ۷ درصد می‌باشد. شکل‌های ۷-ج، ۷-د، ۷-ه و ۷-و به ترتیب مقایسه دقت، حساسیت، معیار اف و ضریب همبستگی متیو را برای دو روش SAAF و ISAAF نمایش می‌دهند. در همه موارد ISAAF نتایج بهتری نسبت به SAAF ثبت کرده است. با توجه به نتایج به‌دست‌آمده می‌توان نتیجه گرفت که روش پیشنهادی با سرعت و دقت بیشتری قادر به شناسایی و حذف کاربران مخرب است که این امر به دلیل تخمین دقیق اعتماد اولیه می‌باشد.



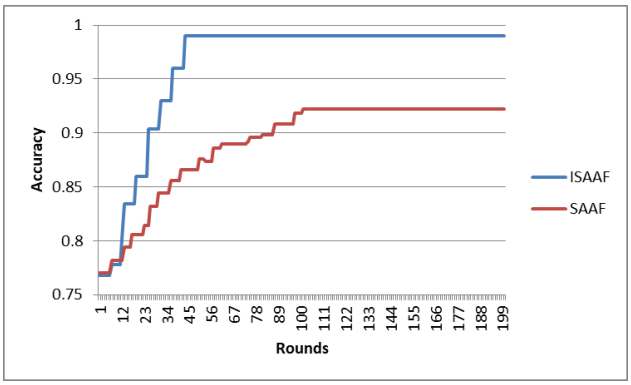
شکل ۵: میزان صحت با حدود آستانه متفاوت در ISAAF.



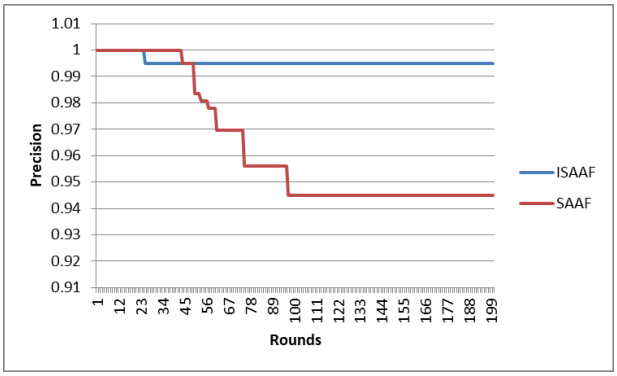
شکل ۶: میزان صحت با افزایش درصد کاربران مخرب در ISAAF.



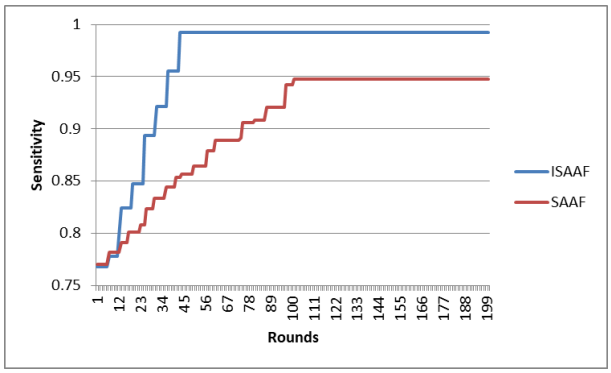
الف- مقایسه زمان فعالیت کاربران مخرب



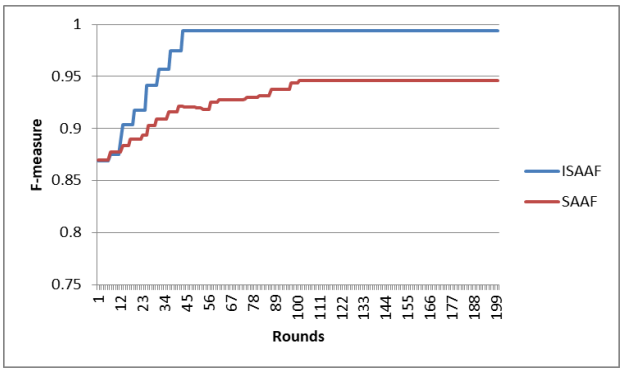
ب- مقایسه میزان صحت



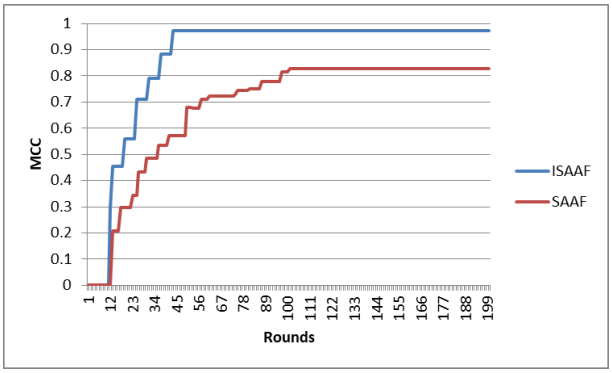
ج- مقایسه میزان دقت



د- مقایسه میزان حساسیت



ه- مقایسه معیار اف



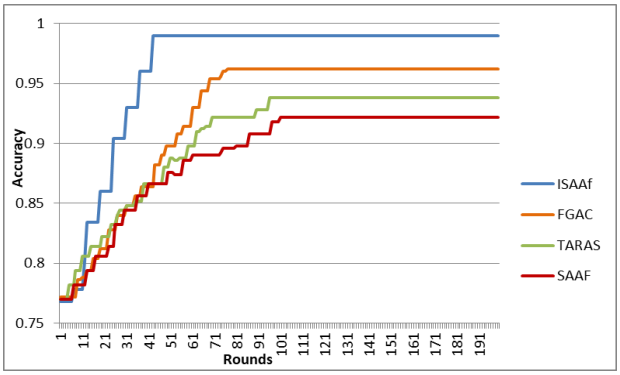
و- مقایسه ضریب همبستگی متیو

شکل ۷: مقایسه SAAF و ISAAF.

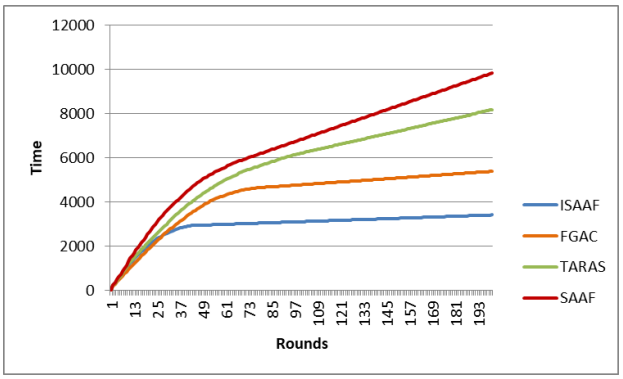
در ادامه این بخش به مقایسه نتایج حاصل از شبیه‌سازی ISAAF با دو روش TARAS[۱۰] و FGAC[۲۶] از حیث صحت تشخیص کاربران مخرب و مقدار زمان فعالیت کاربران مخرب قبل از شناسایی و غیرفعال شدن آن‌ها، پرداخته‌ایم. انتخاب این روش‌ها به دلیل گروه‌بندی هوشمند کاربران و مبتنی بر نقش و اعتماد بودن آن‌ها است. برای انجام مقایسه، سناریوی بخش ۵-۱ با تعداد ۵۰۰ کاربر و با سه نقش مدیر، کارمند و عضو، برای همه روش¬ها با استفاده از JADE و در محیط eclipse شبیه¬سازی و اجرا شد. نتایج به دست آمده در شکل ۸ نمایش داده شده است. شکل ۸-الف میزان صحت را برای هر چهار روش ISAAF، SAAF، TARAS و FGAC، در ۲۰۰ دور و با احتمال مخرب بودن ۲۰٪، نمایش می‌دهد. همان‌طور که در شکل مشاهده می‌شود، در مقایسه با سایر روش‌ها ISAAF مقدار صحت بیشتر را در تعداد دور کمتر به دست می‌آورد. شکل ۸- ب نیز زمان فعالیت کاربران مخرب در سیستم را برای هر چهار روش، در ۲۰۰ دور و با احتمال مخرب بودن ۲۰٪ نشان می‌دهد. در همه روش‌ها زمان فعالیت کاربران مخرب بیشتر از ISAAF بوده است. شکل ۸-ج میزان صحت نهایی را برای هر چهار روش درحالی‌که درصد کاربران مخرب ۱۰، ۲۰، ۳۰، ۴۰ و ۵۰ درصد است، نمایش می‌دهد. هر چهار روش در برابر افزایش تعداد کاربران مخرب مقاوم هستند اما بهترین نتایج برای ISAAF ثبت‌شده‌اند. بهبود نتایج در ISAAF به دلیل استفاده از I-Sharing برای تعیین اعتماد اولیه کاربران و گروه‌بندی هوشمند آن‌ها بر اساس نقش و ویژگی‌های هویتی با استفاده از خوشه‌بندی K-means است.

۶- نتیجه‌گیری

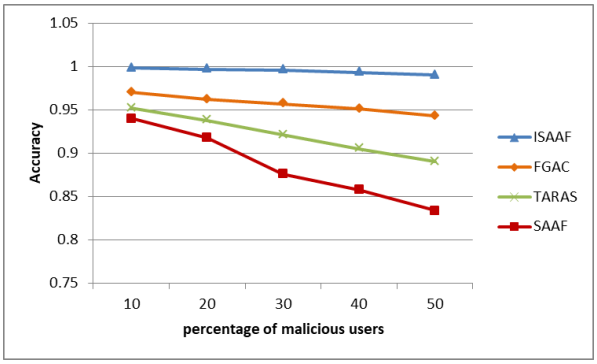
چارچوب مجوز خودتطبیق (SAAF) مؤلفه اصلی اجرای مدیریت خودمختار و یکپارچه‌سازی زیرساخت‌های مجوز است که در آن از مدل مرجع محاسبه خودمختار MAPE-K به‌عنوان راه‌حلی برای شناسایی رفتارهای مخرب و صدور مجوز استفاده‌شده است. مشکل SAAF این است که منابع تصمیم‌گیری آن سیاست‌های تعریف‌شده و سوابق قبلی کاربران است و برای کاربران تازه‌وارد که دارای لیست سوابق نیستند محدودیت خاصی در نظر گرفته نمی‌شود. روش ISAAF که در این مقاله پیشنهادشده از مفاهیم اعتماد و I-sharing برای بهبود SAAF بهره برده است. در این روش هنگامی‌که یک کاربر جدید بدون سابقه قبلی تقاضای



الف- مقایسه میزان صحت.



ب- مقایسه زمان فعالیت کاربران مخرب.



ج- مقایسه صحت با درصدهای مختلف کاربران مخرب.

شکل ۸: مقایسه ISAAF با SAAF، TARAS و FGAC.

دسترسی به سیستم را می‌دهد، می‌توان با توجه به سطح اعتماد اولیه‌اش که از میانگین سطح اعتماد کاربرانی که بیشترین شباهت هویتی را با او دارند (اعضای گروه I-sharing) و بدون هیچ‌گونه تعامل قبلی مجوز دسترسی مناسب را صادر کرد. استفاده از روش یادگیری غیر نظارتی K-means برای ایجاد گروه¬های کاربری و استفاده از ویژگی¬های هویتی کاربران در کنار نقش آن‌ها باعث افزایش دقت در محاسبه اعتماد اولیه و درنتیجه بهبود صحت تشخیص کاربران مخرب شده است. با استفاده از ISAAF به‌طور میانگین می‌توان سطح امنیت و میزان صحت SAAF را بیش از هفت درصد بهبود بخشید همچنین زمان فعالیت کاربران مخرب در سیستم را بیش از ۵۵ درصد کاهش داد. نتایج تجربی حاکی از آن است که ISAAF در مقایسه با روش‌های مشابه نتایج بهتری از حیث صحت یافتن کاربران مخرب و کاهش زمان فعالیت آن‌ها در سیستم تولید می‌کند. مزیت دیگر این روش پیاده‌سازی عناصر حلقه MAPE-K و کاربران با استفاده از عامل‌ها است که موجب استقلال و انعطاف‌پذیری بیشتر سیستم شده است. در این مقاله تعداد گروه‌های I-sharing بایستی از قبل مشخص شوند، اما تعیین دقیق و صحیح آن‌ها کار آسانی نیست و وابسته به تعداد و پراکندگی ویژگی‌ها است. لذا به‌عنوان کارهای آتی، می‌توان از روش‌های خوشه‌بندی که تعداد خوشه‌ها را بر اساس نوع و پراکندگی داده‌ها تعیین می‌کنند استفاده کرد. علاوه بر این بجای استفاده از حد آستانه ثابت می‌توان مقدار حد آستانه را به‌صورت خودتطبیق تعیین کرد تا به‌صورت پویا و با توجه به نوع رفتار و حملات تعیین شود.

مراجع

[1] E. Lara, L. Aguilar, M. A. Sanchez, and J. A. García, "Adaptive security based on mape-k: A survey," in *Applied Decision-Making*: Springer, 2019, pp. 157-183.

[2] A. O'Connor and R. Loomis, "Economic analysis of role-based access control," RTI International2010.

[3] E. Yuan and J. Tong, "Attributed based access control (ABAC) for web services," in *IEEE International Conference on Web Services (ICWS'05)*, 2005: IEEE.

[4] R. McGraw, "Risk-adaptable access control (radac)," in *Privilege (Access) Management Workshop. NIST–National Institute of Standards and Technology–Information Technology Laboratory*, 2009, vol. 25, pp. 55-58.

[5] L. Pasquale, C. Menghi, M. Salehie, L. Cavallaro, I. Omoronyia, and B. Nuseibeh, "SecuriTAS: a tool for engineering adaptive security," in *Proceedings of the ACM SIGSOFT 20th International Symposium on the Foundations of Software Engineering*, 2012, pp. 1-4.

[6] C. Bailey, D. W. Chadwick, and R. De Lemos, "Self-adaptive authorization framework for policy based RBAC/ABAC models," in *2011 IEEE Ninth International Conference on Dependable, Autonomic and Secure Computing*, 2011, pp. 37-44: IEEE.

[7] C. M. Bailey, "Self-adaptive Authorisation Infrastructures," University of Kent, 2015.

[8] E. C. Pinel, A. E. Long, M. J. Landau, K. Alexander, and T. Pyszczynski, "Seeing I to I: a pathway to interpersonal connectedness," *Journal of personality and social psychology*, vol. 90, no. 2, p. 243, 2006.

[9] E. C. Pinel, A. E. Long, and L. A. Crimin, "I-sharing and a classic conformity paradigm," *Social Cognition*, vol. 28, no. 3, pp. 277-289, 2010.

[10] B. Gwak, J.-H. Cho, D. Lee, and H. Son, "Taras: Trust-aware role-based access control system in public internet-of-things," in *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, 2018, pp. 74-85: IEEE.

[11] H. Yang, J.-H. Cho, H. Son, and D. Lee, "Context-aware trust estimation for realtime crowdsensing services in vehicular edge networks," in *2020 IEEE 17th Annual Consumer Communications & Networking Conference (CCNC)*, 2020, pp. 1-6: IEEE.

[12] A. Jøsang and T. Bhuiyan, "Optimal trust network analysis with subjective logic," in *2008 Second International Conference on Emerging Security Information, Systems and Technologies*, 2008, pp. 179-184: IEEE.

[13] C. Bailey, D. W. Chadwick, and R. de Lemos, "Self-adaptive federated authorization infrastructures," *Journal of Computer and System Sciences*, vol. 80, no. 5, pp. 935-952, 2014.

[14] I. Singh and S.-W. Lee, "Self-adaptive and secure mechanism for IoT based multimedia services: a survey," *Multimedia Tools and Applications*, pp. 1-36, 2021.

[15] S. E. A. Rafey, A. Abdel-Hamid, and M. Abou El-Nasr, "CBSTM-IoT: Context-based social trust model for the Internet of Things," in *2016 International Conference on Selected Topics in Mobile & Wireless Networking (MoWNeT)*, 2016, pp. 1-8: IEEE.

[16] K. Kalkan and K. Rasmussen, "TruSD: Trust framework for service discovery among IoT devices," *Computer Networks*, vol. 178, p. 107318, 2020.

[17] C. Boudagdigue, A. Benslimane, A. Kobbane, and M. Elmachkour, "A distributed advanced analytical trust model for IoT," in *2018 IEEE International Conference on Communications (ICC)*, 2018, pp. 1-6: IEEE.

[18] S. Y. Hashemi and F. S. Aliee, "Dynamic and comprehensive trust model for IoT and its integration into RPL," *The Journal of Supercomputing*, vol. 75, no. 7, pp. 3555-3584, 2019.

[19] U. Jayasinghe, G. M. Lee, T.-W. Um, and Q. Shi, "Machine learning based trust computational model for IoT services," *IEEE Transactions on Sustainable Computing*, vol. 4, no. 1, pp. 39-52, 2018.

[20] A. M. Aref and T. T. Tran, "A decentralized trustworthiness estimation model for open, multiagent systems (DTMAS)," *Journal of Trust Management*, vol. 2, no. 1, pp. 1-20, 2015.

[21] Y. Zhang, H. Chen, and Z. Wu, "A social network-based trust model for the semantic web," in *International Conference on Autonomic and Trusted Computing*, 2006, pp. 183-192: Springer.

[22] S. ASHTARI and M. DANESH, "A novel user profile-based fuzzy approach for evaluating trust in semantic web," *IIUM Engineering Journal*, vol. 20, no. 1, pp. 158-176, 2019.

[23] X. Chen and L. Wang, "A cloud-based trust management framework for vehicular social networks," *IEEE Access*, vol. 5, pp. 2967-2980, 2017.

[24] W. Li and H. Song, "ART: An attack-resistant trust management scheme for securing vehicular ad hoc networks," *IEEE transactions on intelligent transportation systems*, vol. 17, no. 4, pp. 960-969, 2015.

[25] F. G. Mármol and G. M. Pérez, "TRIP, a trust and reputation infrastructure-based proposal for vehicular ad hoc networks," *Journal of network and computer applications*, vol. 35, no. 3, pp. 934-941, 2012.

[26] Y. Hou, S. Garg, L. Hui, D. N. K. Jayakody, R. Jin, and M. S. Hossain, "A data security enhanced access control mechanism in mobile edge computing," *IEEE Access*, vol. 8, pp. 136119-136130, 2020.

[27] L. Montrieux, R. de Lemos, and C. Bailey, "Engineering Self-adaptive Authorisation Infrastructures," *arXiv preprint arXiv:1909.13708*, 2019.

[28] J. Park and R. Sandhu, "The UCONABC usage control model," *ACM transactions on information and system security (TISSEC)*, vol. 7, no. 1, pp. 128-174, 2004.

[29] H. Janicke, A. Cau, F. Siewe, and H. Zedan, "Dynamic access control policies: Specification and verification," *The Computer Journal*, vol. 56, no. 4, pp. 440-463, 2013.

[30] M. Serrano, S. van der Meer, J. Strassner, S. De Paoli, A. Kerr, and C. Storni, "Trust and reputation policy-based mechanisms for self-protection in autonomic communications," in *International*

Conference on Autonomic and Trusted Computing, 2009, pp. 249-267: Springer.
[31] S. Bistarelli, F. Martinelli, and F. Santini, "A formal framework for trust policy negotiation in autonomic systems: Abduction with soft constraints," in *International Conference on Autonomic and Trusted Computing*, 2010, pp. 268-282: Springer.
[32] R. De Lemos *et al.*, "Software engineering for self-adaptive systems: A second research roadmap," in *Software Engineering for Self-Adaptive Systems II*: Springer, 2013, pp. 1-32.
[33] J. O. Kephart and D. M. Chess, "The vision of autonomic computing," *Computer*, vol. 36, no. 1, pp. 41-50, 2003.
[34] J. Kramer and J. Magee, "Self-managed systems: an architectural challenge," in *Future of Software Engineering (FOSE'07)*, 2007, pp. 259-268: IEEE.
[35] P. Oreizy *et al.*, "An architecture-based approach to self-adaptive software," *IEEE Intelligent Systems and Their Applications*, vol. 14, no. 3, pp. 54-62, 1999.
[36] A. Ferreira *et al.*, "How to securely break into RBAC: the BTG-RBAC model," in *2009 Annual Computer Security Applications Conference*, 2009, pp. 23-31: IEEE.
[37] S. Adali and J. Golbeck, "Predicting personality with social behavior," in *2012 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining*, 2012, pp. 302-309: IEEE.
[38] K. G. Derpanis, "Mean shift clustering," *Lecture Notes*, p. 32, 2005.
[39] K. Nahiyan, S. Kaiser, K. Ferens, and R. McLeod, "A multi-agent based cognitive approach to unsupervised feature extraction and classification for network intrusion detection," in *International Conference on Advances on Applied Cognitive Computing (ACC). CSREA*, 2017, pp. 25-30.
[40] X. Liu, M. Abdelhakim, P. Krishnamurthy, and D. Tipper, "Identifying malicious nodes in multihop IoT networks using diversity and unsupervised learning," in *2018 IEEE International Conference on Communications (ICC)*, 2018, pp. 1-6: IEEE.
[41] S. Cresci, R. Di Pietro, M. Petrocchi, A. Spognardi, and M. Tesconi, "Fame for sale: Efficient detection of fake Twitter followers," *Decision Support Systems*, vol. 80, pp. 56-71, 2015.
[42] J. B. Schafer, D. Frankowski, J. Herlocker, and S. Sen, "Collaborative filtering recommender systems," in *The adaptive web*: Springer, 2007, pp. 291-324.
[43] J. L. Herlocker, J. A. Konstan, L. G. Terveen, and J. T. Riedl, "Evaluating collaborative filtering recommender systems," *ACM Transactions on Information Systems (TOIS)*, vol. 22, no. 1, pp. 5-53, 2004.
[44] D. M. Powers, "Evaluation: from precision, recall and F-measure to ROC, informedness, markedness and correlation," *arXiv preprint arXiv:2010.16061*, 2020.
[45] M. Jamali and M. Ester, "Trustwalker: a random walk model for combining trust-based and item-based recommendation," in *Proceedings of the 15th ACM SIGKDD international conference on Knowledge discovery and data mining*, 2009, pp. 397-406.
[46] P. Baldi, S. Brunak, Y. Chauvin, C. A. Andersen, and H. Nielsen, "Assessing the accuracy of prediction algorithms for classification: an overview," *Bioinformatics*, vol. 16, no. 5, pp. 412-424, 2000.

پاورقی‌ها:

[1] Insider threats
[2] Role-Based Access Control
[3] Attribute-Based Access Control
[4] Risk-Adaptive Access Control
[5] Secure Tool for Adaptive Security
[6] Self-Adaptive Authorization Framework
[7] Monitor-Analyze-Plan-Execute over a shared Knowledge
[8] Improved SAAF
[9] Self-Protection
[10] Risk-Adaptive Access Control
[11] Secure Tool for Adaptive Security
[12] Fine-Grained Access Control
[13] Resource Usage
[14] Temporal Properties
[15] Trust
[16] Subjective Logic
[17] Confusion matrix
[18] Accuracy
[19] Precision
[20] Sensitivity
[21] F-Measure
[22] Matthew Correlation Coefficient