دوفصل‌نامه علمی منادی امنیت فضای تولید و تبادل اطلاعات (افتا)
سال ۱۴۰۲، جلد ۲۱، شماره ۱ (۱-۱۱)
https://monadi.isc.org.ir

کاربرد مدل ترکیب خطی وزن‌دار- فازی در ارزیابی امنیتی ماژول رمزنگاشتی

زهرا فردوسی[۱] و مرجان بحرالعلوم[۲،*]

[۱] دانشگاه صنعتی امیرکبیر، تهران، ایران
[۲] پژوهشگاه ارتباطات و فناوری اطلاعات، پژوهشکده امنیت، تهران، ایران

اطلاعات مقاله

تاریخچه مقاله:
تاریخ دریافت: ۱۴ فروردین ۱۴۰۱
تاریخ پذیرش: ۱۶ خرداد ۱۴۰۲
انتشار آنلاین: ۱۷ تیر ۱۴۰۲

کلمات کلیدی:
ماژول رمزنگاشتی
معیار ارزیابی
فرآیند تحلیل سلسله مراتبی فازی
مدل ترکیب خطی وزن‌دار

نوع مقاله: مروری

چکیده

امروزه توسعه فناوری اطلاعات و ارتباطات منجر به تولید روزافزون محصولات جدید در این زمینه شده است. یکی از مهمترین محصولاتی که حفاظت از دارایی‌های اطلاعاتی را در سطوح مختلف امنیتی انجام می‌دهد، ماژول رمزنگاشتی است. از این‌رو، ارزیابی امنیتی یک ماژول رمزنگاشتی برای حفاظت در برابر حملات از اهمیت بسزایی برخوردار است. ارزیابی امنیتی یک ماژول رمزنگاشتی نیازمند آگاهی دقیق از نقاط ضعف بالقوه‌ای است که به نقص‌های امنیتی تبدیل می‌شوند. در این مقاله، تصویری جامع از معیارهای ارزیابی امنیتی ماژول رمزنگاشتی مطابق با استانداردهای بین‌المللی موجود (به عنوان مثال FIPS 140-2,3، ISO15408 و PKCS#11) ارائه می‌شود که متناسب با این معیارها و زیرمعیارها می‌توان با استفاده از مدل پیشنهادی و بر اساس ترکیبات خطی با وزن فازی، میزان انطباق این معیارها را برای ارزیابی اندازه‌گیری کرد. همچنین با توجه به این که ساختار هر نوع فرآیند ارزیابی مستلزم هزینه و زمان قابل توجهی است و از یک سو به سیاست‌ها و الزامات کشور و از سوی دیگر به امکانات و کارشناسان بستگی دارد بنابراین معرفی و ارائه‌ی راهکارهایی که به حل چالش‌ها کمک کند، می‌تواند این فرآیند را تسهیل نماید. از این‌رو در بخش پایانی مقاله چالش‌هایی که در فرآیند ارزیابی امنیتی یک محصول همانند ماژول رمزنگاشتی در کشور وجود دارد معرفی می‌شود تا اهمیت مطالعه و تحقیق در این زمینه را تایید کند.

۱ مقدمه

داده‌ها و اطلاعات به عنوان یک دارایی مهم و با ارزش برای هر شخص یا سازمانی به حساب می‌آید و در نتیجه نیازمند ارائه‌ی راهکارهای حفاظتی لازم برای نگهداری است. یکی از روش‌های استاندارد و مناسب به منظور حفظ امنیت داده‌ها در تبادل اطلاعات استفاده از رمزنگاری است. رمزنگاری‌های مبتنی بر کلید عمومی به عنوان یک راهکار امن، نقشی اساسی در ایجاد امنیت در تبادل اطلاعات و خدمات امنیتی مختلف از قبیل اطمینان از صحت داده‌ها، حفظ محرمانگی اطلاعات، احراز هویت (اصالت) و انکارناپذیری و کنترل دسترسی به منابع اطلاعاتی ایفا می‌کند و از این‌رو زیرساخت‌ها و اجزای مورد نیاز در پیاده‌سازی آن از اهمیت بسزایی برخوردار است. انجام نظارت بر فرآیند ارزیابی و ایجاد اطمینان از صحت نتایج در سطوح مختلف امنیتی به منظور صدور مجوز فعالیت برای یک محصول با معرفی زیرساخت‌ها و الزامات مورد نیاز امکان‌پذیر است. از این‌رو مؤسسات و سازمان‌های مختلفی در سراسر جهان در حال تدوین و به‌روز رسانی این الزامات در قالب یک استاندارد هستند. به عنوان مثال مؤسسه NIST به عنوان یکی از مؤسساتی که مسئولیت تدوین استانداردها و الزامات امنیتی برای سیستم‌های اطلاعات فدرال آمریکا را به عهده گرفته است. این مؤسسه مجموعه استانداردهایی را با عنوان

*نویسنده مسئول
آدرس‌های رایانامه: ferdosi@aut.ac.ir (زهرا فردوسی)، bahrololum@itrc.ac.ir (مرجان بحرالعلوم)

استانداردها و الزامات FIPS ارائه می‌کند که سازمان‌های اجرایی دولت فدرال ملزم به رعایت آن‌ها است. مجموعه استاندارد FIPS140 به عنوان یک معماری امنیتی برای مدل OSI است که روشی اصولی برای تعریف و تأمین الزامات امنیتی ارائه می‌کند و قادر است دیدی کلان از مسائل امنیتی عنوان شده در شبکه را برای متخصصان این حوزه فراهم کند. به طور خاص دو نسخه‌ی FIPS140-2 و FIPS140-3 به ارائه‌ی الزامات امنیتی و اصطلاحات پیاده‌سازی ماژول رمزنگاشتی (شامل پیاده‌سازی داخل یک ماژول رمزنگاشتی و طرح‌های رمزنگاشتی پیشنهاد شده توسط NIST) پرداخته است [۱] و [۲]. اهمیت یک ماژول رمز نگاشتی در فرآیند اثبات هویت تعریف می‌شود؛ این فرآیند باید به گونه‌ای طراحی شود که از یک سو دسترسی کاربر برای سیستم به آسانی ممکن باشد و از سوی دیگر برای شخصی که مجاز به دسترسی نیست، تا حد ممکن دشوار باشد. در واقع اکثر مردم با چالش اثبات هویت به منظور احراز هویت روبرو هستند به این دلیل که محافظت از کلیدهای رمزنگاری در قالب یک زیرساخت امنیتی از اهمیت بسزایی برخوردار است و مدیریت امن چرخه حیات کلیدها و محافظت مداوم از آن‌ها نیازمند استفاده از ابزاری به نام ماژول‌های امنیتی رمزنگاشتی (سخت افزاری یا نرم افزاری) است که قادر باشند فرآیند احراز هویت را تسهیل کنند. به دلیل حساسیت موضوع استانداردهایی جهانی جهت سنجش امنیت و اعطای گواهینامه امنیتی برای این ماژول‌ها تدوین شده است.

از این رو در این مقاله سعی شده است تصویری جامع از معیارهای ارزیابی امنیتی ماژول رمزنگاشتی متناسب با استانداردهای موجود جهانی ارائه شود تا با مدل پیشنهادی، فرآیند ارزیابی و محاسبه‌ی درست درصد انطباق این معیارها تسهیل شود. ساختار هر نوع ارزیابی مستلزم صرف هزینه و زمان قابل توجهی است که از طرفی منوط به سیاست‌ها و الزامات حاکم بر کشور و از طرفی دیگر وابسته به امکانات و افراد متخصص است. از این‌رو ارائه‌ی راهکارهایی که به حل چالش‌ها کمک کند اهمیت مطالعه و تحقیق در این حوزه را تأیید می‌کند زیرا در حال حاضر، اطلاعات کامل و جامعی راجع به معیارهای گوناگون و تعیین ارجحیت آن‌ها در فرآیند ارزیابی برای انواع محصولات حوزه‌ی افتا موجود نمی‌باشد. بنابراین، هر گونه اظهار نظر منطقی راجع به کیفیت و کمیت معیارهای موجود و همچنین کامل بودن آن‌ها نمی‌تواند جامع و دقیق باشد.

۲ اهمیت ماژول رمزنگاشتی

به طور کلی دلیل عمده‌ای که باعث شده است استانداردهایی پیرامون ماژول‌های رمزنگاشتی مطرح شود قابلیت‌هایی شامل تضمین محرمانگی، صحت، انکارناپذیری، احراز هویت و غیره است که تجهیزات مجهز به این ماژول‌ها فراهم می‌کنند. در ماژول رمزنگاشتی اطلاعات حساس و محرمانه‌ی کاربران نظیر کلیدهای رمزنگاشتی ذخیره و نگهداری می‌شود. همچنین انجام عملیات و سازوکارهای مختلف رمزنگاشتی توسط ماژول‌ها امکان‌پذیر است. ماژول‌های رمزنگاشتی ممکن است به صورت سخت‌افزاری، نرم‌افزاری یا ترکیبی از نرم‌افزار و سخت‌افزار، پیاده‌سازی

شکل ۱. موجودیت ماژول رمزنگاشتی

شوند که با توجه به خاصیت رمزنگاشتی بودن قادرند تابعی رمزگذاری را در قالب الگوریتمی برای هدف مورد نظر اجرا کنند (شکل ۱). در یک ماژول رمزنگاشتی علاوه بر نرم‌افزار لازم برای اجرای تابع، یک کلید مخفی نیز در درون آن‌ها ذخیره می‌شود. ماژول‌های رمزنگاری معمولاً از نظر ظاهر فیزیکی ایمن هستند و به مهاجم اجازه دسترسی به ورودی دستگاه داده نمی‌شود. تنها بخشی که مهاجم می‌تواند حمله را پیاده‌سازی کند، خروجی ماژول است.

با توجه به اینکه تضمین کیفیت یک ماژول، مبتنی بر پیاده‌سازی آن بر اساس یک استاندارد است. استانداردهای مختلفی شامل معیارها و الزامات امنیتی برای ماژول‌های رمزنگاشتی توسط سازمان‌ها و مؤسسات مختلفی در جهان تدوین شده و مورد استفاده قرار می‌گیرد. البته لازم به ذکر است برای پیاده‌سازی درست هر استاندارد در ابتدا نیاز است، زیرساخت‌های مورد نیاز اجرایی نمودن آن ایجاد شده و سپس از آن استفاده کرد. درکشورهایی که با محدودیت‌هایی در تأمین زیرساخت‌های لازم در حوزه‌های مختلف ICT مواجه هستند نمی‌توان چنین ادعا کرد که یک استاندارد بین‌المللی به طور کامل قابل پیاده‌سازی و اجرا است. لذا چالش عدم وجود استانداردهای ملی (بومی‌سازی شده) متناسب با توانایی کشور از جمله نیازهایی است که باید در حوزه قوانین به تصویب برسد تا با به‌کارگیری دانش به‌روز و نیز رصد و پایش اقدامات سایر کشورها بتوان استاندارد ملی ارائه کرد و به مرحله تکامل رساند.

۳ بررسی استانداردهای مرتبط با ماژول رمزنگاشتی

همان‌طور که اشاره شد نیاز به دستورالعمل‌ها و الزاماتی یکپارچه به منظور انتخاب و پیاده‌سازی راهکارهای مناسب برای حفاظت از اطلاعات منجر شد تدوین استانداردها و الزامات در حوزه امنیت اطلاعات صورت پذیرد. درحال حاضر در دنیا قوانین و الزاماتی در قالب استاندارد پیاده‌سازی ماژول‌های رمزنگاشتی تدوین شده است.

به عنوان مثال نسخه اولیه مجموعه استانداردهای FIPS140 شامل پیاده‌سازی الگوریتم رمزنگاری DES در ماژول‌های رمزنگاشتی است. نسخه دوم این استاندارد، شامل الزامات امنیتی برای ارزیابی و چهار سطح امنیتی برای پیاده‌سازی ماژول‌های رمزنگاشتی است. نسخه سوم استاندارد، شامل سطح امنیتی جدید (سطح پنجم) و الزامات امنیتی برای ارزیابی ماژول‌های رمزنگاشتی نرم‌افزاری و اصلاحات پیاده‌سازی آن‌ها

در شکل ۲ نشان داده شده است.

در سازمان بین المللی استانداردسازی (ISO) و کمیسیون بین‌المللی الکتروتکنیک (IEC) (به صورت جداگانه و مشترک) مجموعه‌ای از استانداردها برای ارزیابی تدوین شده است که استاندارد ایزو 15408 یکی از معروف‌ترین آن‌ها است. به طور کلی این استاندارد شامل سه بخش است [۳]. بخش اول آن شامل مفاهیم و دستورالعمل‌هایی کلی است که ارزیابی امنیت فناوری اطلاعات را مشخص نموده و نمونه‌ای کلی از مراحل ارزیابی را نشان می‌دهد. قسمت دوم این استاندارد شامل الزامات امنیتی و کارکردی به کلاس‌ها و مؤلفه‌ها است. قسمت سوم این استاندارد نیز شامل مجموعه‌ای از مؤلفه‌های تضمین و همچنین معیار ارزیابی برای پروفایل‌های محافظتی و اهداف امنیتی است. این استاندارد مورد پذیرش در سطح جهانی است و کشورهای ایالات متحده، انگلیس و کانادا بنیان‌گذاران اصلی پذیرش این استاندارد بودند و با رسمیت یافتن این استاندارد در سایر کشورها از جمله آلمان، فرانسه، هلند و دیگر کشورها، جایگاه بین‌المللی خود را در قالب استانداردی جهانی بدست آورد [۴].

استاندارد ایزو 15408 در چهار فصل تدوین شده است:

(۱) معرفی و مدل کلی شامل تشریح ملزومات اصلی یعنی هدف امنیتی و پروفایل حفاظتی (شامل الزامات امنیتی فناوری اطلاعات مربوط به نوع خاصی از فناوری محصول است که الزامات کارکردی و تضمین امنیتی را توسط محصول مشخص می‌کند)،
(۲) توصیف مؤلفه‌های کارکرد امنیتی [۱] (که از این مؤلفه‌ها می‌توان در طراحی یک محصول بهره گرفت)،
(۳) توصیف مؤلفه‌های تضمین امنیت [۲] و
(۴) اصول مشترک در ارزیابی امنیت IT جهت بررسی وجود یا عدم وجود هر یک از مؤلفه‌های تضمین امنیت تدوین شده است.

یکی از مزایای مهم استاندارد 15408 سند تنظیم بازشناسی معیار مشترک CCRA [۳] است [۵] که در حال حاضر در چندین کشور مورد تأیید قرار گرفته است. بر اساس سند CCRA هر ارزیابی که در یکی از کشورهای عضو اجرا می‌شود، تا سطح امنیتی چهارم [۴] (4EAL) مورد تأیید سایر کشورها نیز قرار می‌گیرد. این ویژگی برای مصرف‌کنندگان به معنی وجود مجموعه بزرگی از محصولات امنیتی IT تولید شده توسط کشورهای مختلف است که توانایی تأمین نیازهای آن‌ها را دارد. از دیگر استانداردهای مربوط به الزامات امنیتی برای ماژول‌های رمزنگاشتی می‌توان به استاندارد ایزو 19790 اشاره کرد که شامل الزامات امنیتی برای یک ماژول رمزنگاشتی استفاده شده در یک سیستم امنیتی است که از اطلاعات حساس محافظت می‌کند [۶]. لازم به ذکر است که این استاندارد از FIPS140-2 برگرفته شده اما به صورت مستقل ارائه شده است. یکی دیگر از استانداردهای ایزو که در سال ۲۰۰۸ منتشر شده استاندارد ایزو 24759 است که به الزامات و شیوه‌های تست ماژول رمزنگاشتی پرداخته و در استاندارد FIPS140-3 به آن ارجاع شده است [۷]. این استاندارد روش‌های مورد استفاده در آزمایشگاه‌های تست را مشخص می‌کند که برای بررسی و تست میزان انطباق ماژول رمزنگاشتی با الزامات مشخص شده در ایزو 19790 ضروری است. در واقع این روش‌ها به منظور ایجاد درجه بالایی از تطبیق واقعیت در طی مراحل آزمایش و اطمینان از سازگاری در آزمایشگاه‌های تست، ارائه شده است. این استاندارد همچنین به الزاماتی پرداخته است که فروشندگان باید در خصوص محصول خود به آزمایشگاه‌ها توضیح دهند. برای نشان دادن انطباق ماژول‌های رمزنگاشتی با الزامات مشخص شده در ایزو 19790 سند پشتیبان معرفی می‌گردد که فروشندگان محصولات می‌توانند با تکمیل این سند پشتیبان این امکان را فراهم می‌کند تا قبل از انجام آزمایش‌ها در آزمایشگاه، ماهیت درونی، ماژول‌های تولیدی برای تأیید الزامات ایزو 19790 بررسی شود. مجموعه دیگری از استاندارد (مجموعه‌ای شامل ۱۵ استاندارد) که هم به موضوع رمزنگاری کلید عمومی و هم به موضوع ماژول‌های رمزنگاشتی می‌پردازد، استانداردهای رمزنگاری کلید عمومی PKCS [۵] معروف به استانداردهای مخصوص فروشنده است که با همکاری RSA Laboratories (بخشی از RSA Data Security Inc) تهیه شده است [۸]. این استانداردها به منظور تسریع در استقرار کلید عمومی رمزنگاری تهیه شده و به طور گسترده‌ای در عمل اجرا و به‌روز می‌شود. مجموعه استاندارد PKCS در بخش عمده‌ای از استانداردهای رسمی همانند استانداردهای 9ANSIX [۶] [۹] و IETF [۷] (مجموعه استانداردهای مربوط به تکنیک‌ها و توسعه رمزنگاری کلید عمومی [۱۰]) استفاده شده است. به طور خاص در استاندارد شماره ۱۱، استانداردی برای به‌کارگیری واسط ماژول رمزنگاشتی در سیستم‌های نرم‌افزاری است که با ارائه یک واسط (رابط) برنامه نویسی کاربردی (API) به نام «Cryptoki» قادر است انواع داده‌ها و توابع موجود در برنامه را که نیاز به خدمات رمزنگاری دارد برای دستگاه‌های نگهدارنده و یا پردازنده اطلاعات رمزنگاری مشخص کرده و یک نمای مشترک با نام «توکن رمزنگاشتی» به آن برنامه‌ها عرضه کند. به دلیل جامعیت، سازگاری، تعامل‌پذیری نسبتاً بالا و نیز استقبال جهانی، نسخه سوم از استاندارد PKCS#11 [۸] به عنوان استاندارد و معیار اصلی سنجش کارکرد ماژول رمزنگاشتی در نظر گرفته شده است [۱۱]. در حالت کلی با توجه به بررسی استانداردها می‌توان چنین نتیجه‌گیری کرد که عمده‌ی تلاش‌های نهادهای استاندارد بین‌المللی و سایر سازمان‌ها و مؤسسات، متمرکز بر همکاری در به اشتراک گذاشتن تجارب ارزیابی و جلوگیری از تکرار آن‌ها است. در استانداردهای پیرامون ماژول رمزنگاشتی حوزه‌های مختلفی

[۴] سطح اطمینان ارزیابی (EAL) دارای هفت سطح است که برای یک محصول یا سیستم فناوری اطلاعات پس از اتمام ارزیابی امنیتی و براساس استاندارد ارزیابی معیارهای مشترک یک درجه عددی اعمال می‌شود. به عنوان مثال سطح چهارم آن مربوط به بررسی و ارزیابی طراحی و روش آزمایش است.

[1] Security Functional Components [2] Security Assurance Components [3] Common Criteria Recognition Arrangement (https://www.niap-ccevs.org/Ref/CCRA.Partners.cfm)

[5] Public Key Cryptography Standards (http://www.rsasecurity.com/rsalabs/pkcs) [6] ANSI X9 (https://x9.org/standards/standards-store) [7] IETF (Available: https://www.ietf.org/standards) [8] PKCS #11 (https://docs.oasis-open.org/pkcs11/pkcs11-profiles/v3.0/pkcs11-profiles-v3.0.html)

الزامات امنیتی						
	دارای نرم افزاری که محافظت بر پایه‌ی رمزنگاری قوی را برای شناسایی و جلوگیری از افشای و اصلاح پارامترهای امنیت عمومی و همچنین پارامترهای امنیتی حیاتی در هنگام غیرفعال بودن ماژول انجام می‌دهد	–	–	–	–	✔
	محافظت در برابر تغییرات محیطی	–	–	–	✔	✔
	امحای نفوذ	–	–	–	✔	✔
	احراز هویت شناسه محور	–	–	✔	✔	✔
	حفاظت پیشرفته از کلیدهای خصوصی و مخفی	–	–	✔	✔	✔
	تشخیص نفوذ و واکنش به آن	–	–	✔	✔	✔
	آشکارسازی نفوذ و پشتیبانی از ساز و کار احراز هویت نقش محور	–	✔	✔	✔	✔
	حداقل یک الگوریتم رمزنگاشتی یا تابع امنیتی پیاده‌سازی شده (رویکرد کنترل دسترسی به واحدهای اطلاعاتی حیاتی موجود در ماژول)	✔	✔	✔	✔	✔
	سطوح امنیتی	۱	۲	۳	۴	۵

FIPS 140-2

FIPS 140-3

شکل ۲. الزامات و سطوح امنیتی استانداردهای FIPS 140-2 و FIPS 140-3 برای بکارگیری یک ماژول رمزنگاشتی

شکل ۴. انواع ورودی و خروجی‌های (پذیرفته، رد و مشروط) یک تابع ارزیابی با رویکرد قابل پذیرش و قابل استفاده بودن

۴ فرآیند ارزیابی

شناخت «ارزیابی» ناشی از سیاستی است که در مواجهه با اجرای آن اتخاذ می‌گردد. در حالت کلی می‌توان گفت در فرآیند ارزیابی سعی بر این است که روشی اصولی و قوی برای اندازه‌گیری موضوعات و مفاهیم ارائه شود تا در تصمیم‌گیری و درک آنچه قابل قبول است استفاده شود. اگر در اولویت بندی و شناخت مواردی که قابل ارزیابی است تمرکز کافی صورت نگیرد جدای از اتلاف منابع و هزینه‌ها، خروجی‌هایی حاصل می‌شود که ضعف در اثر بخشی و بازده دارند. در حوزه ارتباطات و فناوری اطلاعات (ICT) می‌توان ارزیابی را به عنوان تابعی در نظر گرفت که با معیارهای امکانپذیر بودن، قابل پذیرش و قابل استفاده بودن، قادر است از ورودی، خروجی‌هایی در سه حالت پذیرفته شده، رد شده و مشروط ارائه کند (شکل ۴).

شکل ۳. حوزه‌های کلی پیشنهادی پیرامون ارزیابی ماژول

در نظر گرفته شده که متناسب با آن‌ها، الزاماتی برای پیاده‌سازی مطرح می‌شود. در این مقاله تلفیقی از حوزه‌های مختلف موجود در استانداردهای ماژول برای استخراج الزامات به صورت شکل ۳ نشان داده شده است.

ارزیابی پیرامون محصولات ICT و اجرای زیرساخت‌های مناسب برای تسهیل این فرآیند، چند سالی است در ایران با همکاری سازمان فناوری اطلاعات و افتای ریاست جمهوری در حال انجام است. تعریف سطوح امنیتی مختلف مطابق با استانداردهای موجود، اولین اقدامی است که صورت گرفته و با توجه به توانایی‌های موجود تاکنون برای محصولات شرکت‌های داخلی بررسی شده است و تاییدیه این محصولات، با ارائه گواهینامه‌های معتبر از سوی این نهادها صورت می‌گیرد. با توجه به پیشرفت روزافزون فناوری و محصولات، لازم است ارزیابی‌ها دقیق‌تر گردد و بلوغی برای دستیابی به ارزیابی‌های دقیق‌تر و ورود به سطوح امنیتی بالاتر صورت گیرد زیرا که حملات عمیق‌تر، دقیق‌تر و پیچیده‌تر شده است. از این‌رو تاکنون محورهایی برای ارزیابی محصولات ICT ارائه شده که شامل: امنیتی، کارکردی، قابلیت اطمینان، استفاده، نگهداری و پایداری است.

۵ معیارهای ارزیابی ماژول

مهم‌ترین بحث در برخورد با ارزیابی هر محصول یا خدمت، گام اول شناخت جنبه‌های تحلیلی محصولات یا خدمات در راستای میزان در دسترس بودن اطلاعات مربوط به آن‌ها در بحث کارکرد، نگهداری، تعمیر و اندازه‌گیری میزان انطباق با اصول فنی و عملکردی است. گام دوم شناسایی دقیق ابزار و تجهیزات لازم برای ارزیابی محصولات یا خدمات است و در گام آخر بررسی قابلیت ارتقاء ویژگی‌های آن‌ها است که در قالب جدولی خروجی این ارزیابی قابل نمایش است.

در فرآیند سیاست‌گذاری ارزیابی باید بررسی شود که هدف از ارزیابی، استخراج اطلاعات به منظور یادگیری است یا استخراج اطلاعات به منظور پاسخگویی در مواجه با چالش‌ها و مشکلات محصولات و خدمات. یکی از چالش‌هایی که در یک فرآیند ارزیابی وجود دارد علاوه بر چگونگی انجام آن، نحوه محاسبه‌ی دقیق درصد انطباق معیارهای ارزیابی با واقعیت است. از این‌رو لزوم به کارگیری روش‌های تصمیم‌سازی جهت محاسبه‌ی درست میزان انطباق ارزیابی ضروری می‌شود.

هدف عمده‌ی این مقاله نیز ارائه‌ی روشی برای اندازه‌گیری ارزیابی مبتنی بر تصمیم‌گیری چند معیاره با استفاده از مدل ترکیب خطی وزن‌دار- فازی[1] است. به عنوان مثال حوزه‌های مورد نیاز و تاثیرگذار بر ارزیابی امنیتی یک ماژول رمزنگاشتی برگرفته از استانداردهای موجود FIPS140-2، 3-140 و ایزو 19790 در شکل ۵ شناسایی و ترسیم شده است که در ادامه با معرفی معیارها و زیرمعیارها مرتبط به هر حوزه به ارائه‌ی مدل پیشنهادی برای اندازه‌گیری درصد انطباق ارزیابی امنیتی با توجه به این معیارها پرداخته شده است. از آنجایی که میزان تاثیر معیارهای حاصل از ارزیابی برای هر محصول با یکدیگر برابر نیست بنابراین با نظر سنجی از کارشناسان خبره می‌توان درجه‌ی اهمیت و ارزش معیارها را استخراج کرده و درصد ارجحیت آن‌ها را در ارزیابی هر محصول محاسبه کرد. برای محاسبه‌ی درجه اهمیت یا همان وزن مناسب برای هر معیار در این مقاله از روش تحلیل سلسله مراتبی فازی (FAHP[2]) استفاده شده که با کمک نرم‌افزارهای تحلیل سلسله مراتبی فازی موجود و یا تحلیل شبکه‌ای (ANP[3]) قابل انجام است [۱۲-۱۶]. در این مقاله با استفاده از مدل پیشنهادی می‌توان اندازه‌گیری درصد انطباق را برای هر یک از معیارهای فرآیند ارزیابی تسهیل و تدقیق کرد. بررسی میزان اهمیت و درصد انطباق نزدیک به واقعیت مزایایی از جمله: اثبات ادعای پدیدآورنده‌ی یک محصول، شفاف‌سازی در رد یا پذیرش یک محصول توسط ناظرین، بهبود عملکرد کیفی و کمّی آزمایشگاه‌ها و پدیدآورنده‌ها، حذف هزینه‌های اضافی در آزمون مجدد یا نظارت مجدد و ارائه‌ی خدمات موثر در تجارت (در شرایط برابر) را در بر خواهد داشت.

۶ مرور کلی بر فرآیندهای تحلیلی

۱.۶ تحلیل سلسله مراتبی

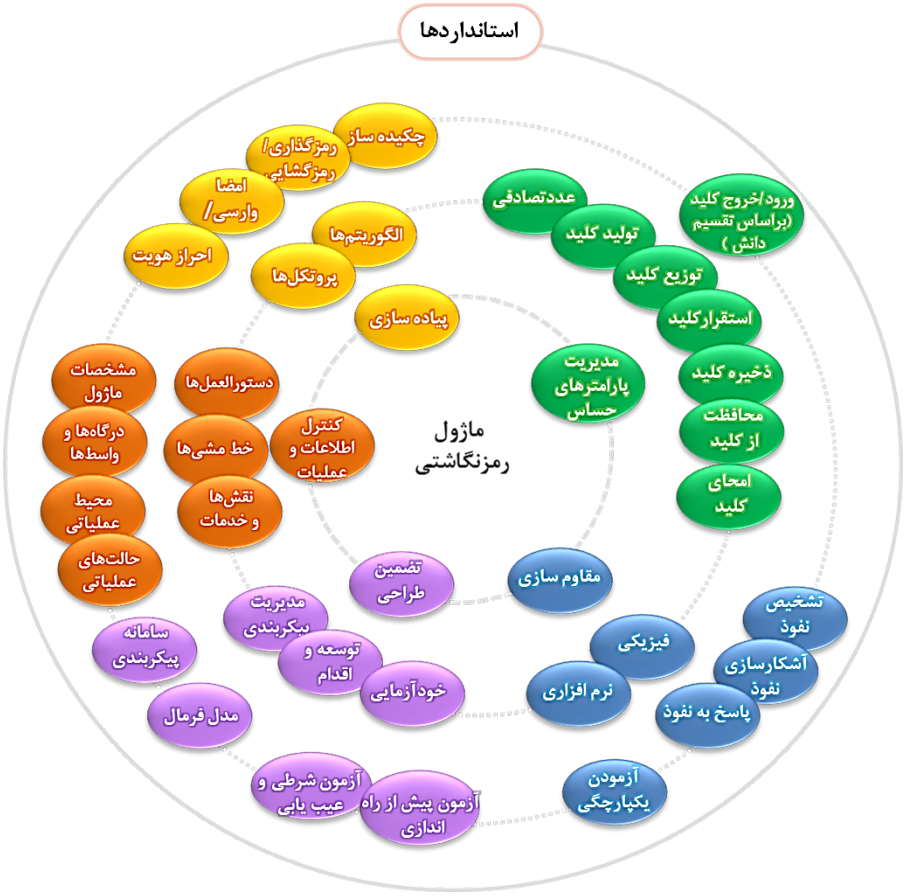
فرآیند تحلیل سلسله‌مراتبی (AHP) که در دهه هفتاد میلادی توسط Saaty[4] پیشنهاد شد [۱۷؟ -۱۹]. این روش یکی از روش‌های تصمیم‌گیری چند معیاره است که با تشکیل یک سلسله‌مراتب برای تصمیم‌گیری، امکان تعیین معیارهای تصمیم‌گیری بهینه را فراهم می‌سازد. یکی از مهمترین اجزای ارزیابی، تعیین معیارها با ضریب اهمیت دقیق است، انتخاب نادرست معیارهای کلیدی در هر حوزه ارزیابی یکی از علت‌های بروز شکست در پیاده‌سازی ارزیابی است. در روش AHP، ورودی اصلی، درک متخصصان یا عامل ذهنی در تصمیم‌گیری آن‌ها است این ورودی به طور قابل ملاحظه‌ای بر عدم قطعیت و تردید بر صحت نتایج بدست آمده تأثیر می‌گذارد. از این‌رو یکی از راهکارهایی که برای غلبه بر نوع کاستی‌ها در فرآیند تحلیل سلسله مراتبی پیشنهاد می‌شود به‌کارگیری نظریه فازی است که با ارائه‌ی بازه‌ای به جای یک ارزش با مقدار ثابت، تصمیم‌گیری را برای فرد تصمیم‌گیرنده راحت‌تر می‌سازد [۲۰].

۲.۶ تحلیل سلسله مراتبی فازی

تفکر فازی با الهام از فلسفه شرقی، جهان را همان گونه که هست معرفی می‌کند. فازی بودن، هر پدیده یا موجودیت به معنای سازگاری با طبیعت و ماهیت چندارزشی بودن است. در یک نظام فازی همه قواعد درجه‌ای از درستی یا نادرستی را در خود دارند که در نتیجه‌ی نهایی تأثیر می‌گذارند. مجموعه‌های فازی یک شروع سهل و آسان برای ساخت یک چارچوب مفهومی را فراهم می‌کنند و در زمینه‌ی الگوهای تحلیلی و طبقه‌بندی، طیف وسیعی را شامل می‌شوند. منطق فازی در روش تحلیل سلسله مراتبی فازی (FAHP)، موجب سازگاری بیشتر و تصمیم‌گیری نزدیک به واقعیت خواهد شد. در این روش نیز مشابه تحلیل سلسله مراتبی از توانایی افراد متخصص در تشکیل درخت سلسله مراتبی معیارها استفاده شده و سپس با به‌کارگیری اعداد فازی (اعداد فازی مثلثی یا اعداد فازی

[1] Fuzzy-Weighted Linear Combination (FWLC) model

[2] Fuzzy Analytic Hierarchy Process [3] Analytical Network Process [4] Thomas L. Saaty



شکل ۵. تصویری جامعی از معیارهای قابل ارزیابی امنیتی در یک ماژول رمزنگاشتی (برگرفته از استانداردهای موجود)

ذوزنقه‌ای) و تشکیل ماتریس مقایسه دوتایی برای هر سطح در سلسله مراتب معیارها درجه اهمیت آن‌ها اندازه‌گیری شده و به عنوان وزن معیارها معرفی می‌گردد [۲۱].

۳.۶ تحلیل شبکه‌ای

فرایند تحلیل شبکه‌ای (ANP) یکی دیگر از روش‌های تصمیم‌گیری چند معیاره است که با جایگزینی «شبکه» بجای «سلسله مراتب» فرایند تحلیل سلسله مراتبی را بهبود می‌بخشد. در فرآیند تحلیل سلسله مراتبی، وابستگی درونی معیارها و زیرمعیارها در نظر گرفته نمی‌شود اما در ANP وابستگی و رابطه موجود میان معیارها و زیرمعیارهای هر معیار، ساختاری شبکه‌ای ایجاد می‌کند که همان وجه تسمیه این روش است. اساس تعیین اولویت در این روش نیز مقایسه‌های دوتایی است اما ANP هیچ ساختار خاص و قابل پیش بینی ندارد. در AHP وزن نهایی براساس ضرب ساده اهمیت هر عنصر در خوشه بالایی خود بدست می‌آید اما در ANP با محاسبه سوپرماتریس [1] حد وزن نهایی عناصر بدست خواهد آمد [۲۲].

۷ مدل پیشنهادی

۱.۷ مدل ترکیب خطی وزن‌دار-فازی

در منطق فازی هر موضوع یا مفهومی دارای یک درجه‌ی عضویت است، اطلاعات و داده‌های هر سیستم یا فرآیند را می‌توان به صورت مجموعه‌ای از متغیرها در قالب ترکیبات خطی وزن‌دار فازی بیان کرد.

در مدل ترکیب خطی وزن‌دار (WLC) هر متغیر در ابتدا استاندارد شده سپس به وزن مربوطه ضرب و سپس نتایج تمام متغیرها با همدیگر جمع می‌شود، روش WLC یک میانگین‌گیری است که با تداوم بخشیدن به فضای تصمیم‌گیری دقیقاً یک حالت میانه (حداقل به حداکثر) پیدا می‌کند. همانگونه که بیان شد وجود معیارهای مختلف و گاه متضاد برای تصمیم‌گیری، کاربرد روش‌های چند متغیره را در ارزیابی آن‌ها الزامی می‌سازد. در این مقاله با استفاده از فرآیند تحلیل سلسله مراتبی فازی مبتنی بر مدل ترکیب خطی وزن‌دار محاسبات درجه اهمیت معیارهای ارزیابی برای یک ماژول رمزنگاشتی با استفاده از محیط‌های نرم‌افزاری Expert Choice و Matlab انجام شده است.

طی این فرآیند ابتدا معیارهای مورد نیاز و تاثیرگذار برای ارزیابی امنیتی یک ماژول رمزنگاشتی و همگرا با استانداردهای بین‌المللی در

[1] Supper matrix

جدول ۱. طیف پنجگانه AHP فازی

عدد نظیر	مقیاس زبانی	عدد فازی مثلثی	معکوس عدد فازی مثلثی
۱	اهمیت یکسان	$(1,1,1)$	$(1,1,1)$
۲	کمی مهم	$(\frac{1}{2},1,\frac{3}{2})$	$(\frac{2}{3},1,2)$
۳	مهمتر	$(1,\frac{3}{2},2)$	$(\frac{1}{2},\frac{2}{3},1)$
۴	خیلی مهمتر	$(\frac{3}{2},2,\frac{5}{2})$	$(\frac{2}{5},\frac{1}{2},\frac{2}{3})$
۵	کاملاً مهمتر	$(2,\frac{5}{2},3)$	$(\frac{1}{3},\frac{2}{5},\frac{1}{2})$

جدول ۲. یک نمونه پرسشنامه ارزشگذاری پرشده توسط یک کارشناس

معیار i	ارزش گذاری معیار i نسبت به j					معیار j
مدیریت پارامترهای حساس	5	4	3	2	1	مقاوم‌سازی
مدیریت پارامترهای حساس	5	4	3	2	1	پیاده‌سازی
مدیریت پارامترهای حساس	5	4	3	2	1	کنترل اطلاعات و عملیات
مدیریت پارامترهای حساس	5	4	3	2	1	تضمین طراحی
مقاوم‌سازی	5	4	3	2	1	پیاده‌سازی
مقاوم‌سازی	5	4	3	2	1	کنترل اطلاعات و عملیات
مقاوم‌سازی	5	4	3	2	1	تضمین طراحی
پیاده‌سازی	5	4	3	2	1	کنترل اطلاعات و عملیات
پیاده‌سازی	5	4	3	2	1	تضمین طراحی
کنترل اطلاعات و عملیات	5	4	3	2	1	تضمین طراحی

شکل ۵ ترسیم شده است. سپس با طراحی پرسشنامه‌ی ارزشگذاری معیارها و جمع‌آوری نظر افراد متخصص و پیاده‌سازی هفت مرحله‌ی تحلیل سلسله مراتبی فازی (بر اساس روش آنالیز چانگ) درجه اهمیت معیارها در قالب وزن نرمال شده استخراج گردید و در مدل ترکیب خطی وزن‌دار-فازی استفاده شده است.

۲.۷ مراحل روش تحلیل سلسله مراتبی فازی

مرحله ۱: تعیین معیارهای ارزیابی (رسم معیارها و زیرمعیارها در نمودار سلسله مراتبی).

مرحله ۲: تعریف اعداد فازی به منظور انجام مقایسه‌ی دوتایی (جدول ۱ و جدول ۲).

مرحله ۳: تشکیل ماتریس‌های مقایسه دوتایی (این ماتریس‌ها با توجه به اعداد فازی مثلثی پنجگانه تشکیل داده شده است) (جدول ۳).

مرحله ۴: محاسبه‌ی S_i برای هر یک از سطرهای ماتریس‌های مقایسه دوتایی (S_i ارزش اندازه ترکیبی فازی با توجه به iامین معیار).

مرحله ۵: محاسبه‌ی درجه ارجحی S_iها نسبت به همدیگر.

مرحله ۶: محاسبه‌ی وزن‌های معیارها و زیرمعیارها در ماتریس‌های مقایسه دوتایی.

مرحله ۷: محاسبه‌ی وزن بردار نهایی نرمال‌سازی آن

یک نمونه ماتریس مقایسه دوتایی استخراجی از پرسشنامه ارزشگذاری معیارها توسط یک کارشناس به صورت جدول ۲ بدست آمده است.

نتایج محاسباتی که برای تعیین وزن مناسب برای معیارها و زیرمعیارها بر اساس داده‌های ماتریس مقایسه دوتایی انجام شده در جدول ۴ (الف) و (ب) نشان داده شده است. در این مقاله به منظور تعیین معیارهای انتخاب و استخراج وزن‌های مناسب برای این معیارها در ارزیابی ماژول رمزنگاشتی از چندین کارشناس خبره در این زمینه، شامل اساتید دانشگاه و کارشناسان حوزه ارزیابی امنیتی استفاده شده است.

در شکل ۶، سلسله مراتب پنج معیار (۱-مدیریت پارامترهای حساس،

جدول ۳. ماتریس مقایسه‌های دوتایی معیارها بر اساس یک نظر کارشناسی

	مدیریت پارامترهای حساس	مقاوم‌سازی	پیاده سازی	کنترل اطلاعات و عملیات	تضمین طراحی
مدیریت پارامترهای حساس	$(1,1,1)$	$(\frac{1}{2},1,\frac{3}{2})$	$(1,\frac{3}{2},2)$	$(2,\frac{5}{2},3)$	$(2,\frac{5}{2},3)$
مقاوم‌سازی	$(\frac{2}{3},1,2)$	$(1,1,1)$	$(\frac{3}{2},2,\frac{5}{2})$	$(2,\frac{5}{2},3)$	$(2,\frac{5}{2},3)$
پیاده سازی	$(\frac{1}{2},\frac{2}{3},1)$	$(\frac{2}{5},\frac{1}{2},\frac{2}{3})$	$(1,1,1)$	$(1,\frac{3}{2},2)$	$(1,\frac{3}{2},2)$
کنترل اطلاعات و عملیات	$(\frac{1}{3},\frac{2}{5},\frac{1}{2})$	$(\frac{1}{3},\frac{2}{5},\frac{1}{2})$	$(\frac{1}{2},\frac{2}{3},1)$	$(1,1,1)$	$(1,1,1)$
تضمین طراحی	$(\frac{1}{3},\frac{2}{5},\frac{1}{2})$	$(\frac{1}{3},\frac{2}{5},\frac{1}{2})$	$(\frac{1}{2},\frac{2}{3},1)$	$(1,1,1)$	$(1,1,1)$

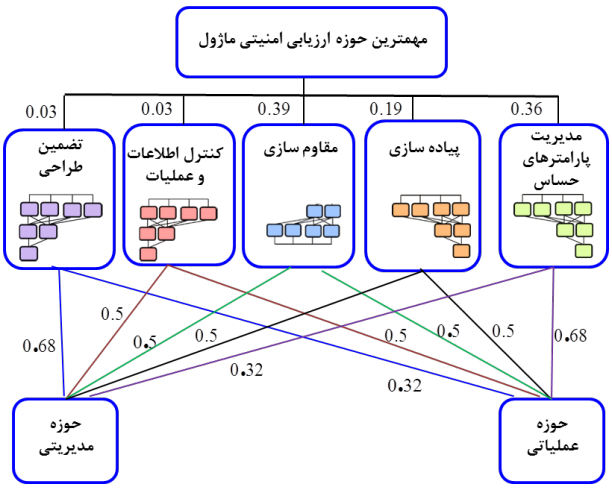
جدول ۴. الف) محاسبات وزن معیارها، ب) پنج ماتریس مقایسه دوتایی به همراه محاسبه‌ی وزن زیرمعیارها

$v(S_i > S_j)$	S_1 مدیریت پارامتر حساس	S_2 مقاوم سازی	S_3 پیاده سازی	S_4 کنترل اطلاعات و عملیات	S_5 تضمین طراحی	min	$normal(w)$
S_1 مدیریت پارامتر حساس		0.94	1	1	1	0.94	0.36
S_2 مقاوم‌سازی	1		1	1	1	1	0.39
S_3 پیاده سازی	0.54	0.48		1	1	0.48	0.19
S_4 کنترل اطلاعات و عملیات	0.15	0.08	0.59		1	0.08	0.03
S_5 تضمین طراحی	0.15	0.08	0.59	1		0.08	0.03

(الف)

	مدیریت پارامترهای حساس	ح مدیریت	ح عملیات	$v(S_1 > S_2)$	$v(S_2 > S_1)$	وزن نرمال
S_1	ح مدیریت		$(\frac{1}{2},\frac{2}{3},1)$	0.46	1	0.32
S_2	ح عملیات	$(1,\frac{3}{2},2)$				0.68
	مقاوم سازی	ح مدیریت	ح عملیات	$v(S_1 > S_2)$	$v(S_2 > S_1)$	وزن نرمال
S_1	ح مدیریت		$(1,1,1)$	1	1	0.5
S_2	ح عملیات	$(1,1,1)$				0.5
	پیاده سازی	ح مدیریت	ح عملیات	$v(S_1 > S_2)$	$v(S_2 > S_1)$	وزن نرمال
S_1	ح مدیریت		$(\frac{2}{3},1,\frac{1}{2})$	1	1	0.5
S_2	ح عملیات	$(\frac{1}{2},1,\frac{3}{2})$				0.5
	کنترل اطلاعات و عملیات	ح مدیریت	ح عملیات	$v(S_1 > S_2)$	$v(S_2 > S_1)$	وزن نرمال
S_1	ح مدیریت		$(\frac{2}{3},1,\frac{1}{2})$	1	1	0.5
S_2	ح عملیات	$(\frac{1}{2},1,\frac{3}{2})$				0.5
	تضمین طراحی	ح مدیریت	ح عملیات	$v(S_1 > S_2)$	$v(S_2 > S_1)$	وزن نرمال
S_1	ح مدیریت		$(1,\frac{3}{2},2)$	1	0.46	0.68
S_2	ح عملیات	$(\frac{1}{2},\frac{2}{3},1)$				0.32

(ب)



شکل ۶. نمودار سلسله مراتب و وزن‌دهی معیارها و زیرمعیارها بر اساس یک نظر کارشناسی

۲- مقاوم‌سازی، ۳-پیاده‌سازی، ۴-کنترل اطلاعات و عملیات و ۵- تضمین طراحی) و دو حوزه مدیریتی و عملیاتی به عنوان زیرمعیارهای فرآیند ارزیابی امنیتی یک ماژول رمزنگاشتی ترسیم شده است و با استفاده از داده‌های حاصل از ماتریس مقایسه دوتایی معیارها و ۵ ماتریس مقایسه دوتایی زیرمعیارها بر اساس نظر یک کارشناس، درجه اهمیت و وزن نرمال‌شده‌ی[۱] نظیر آن‌ها بدست آمده است.

در مرحله نهایی با در نظر گرفتن محاسبه وزن (اهمیت نسبی) معیارها می‌توان وزن نهایی زیرمعیارها را به صورت زیر استخراج کرد:

وزن نهایی حوزه مدیریتی:

$$w_۱ = (۰٫۰۳ \times ۰٫۶۸) + (۰٫۰۳ \times ۰٫۵) + (۰٫۳۹ \times ۰٫۵) + (۰٫۱۹ \times ۰٫۵) + (۰٫۳۶ \times ۰٫۳۲) \approx ۰٫۴۵$$

وزن نهایی حوزه عملیاتی:

$$w_۲ = (۰٫۰۳ \times ۰٫۳۲) + (۰٫۰۳ \times ۰٫۵) + (۰٫۳۹ \times ۰٫۵) + (۰٫۱۹ \times ۰٫۵) + (۰٫۳۶ \times ۰٫۶۸) \approx ۰٫۵۵$$

در هر سطح از ساختار سلسله مراتبی، می‌توان اوزان را به عنوان ضرایب مدل ترکیب خطی وزن‌دار در نظر گرفت و درصد انطباق را متناسب با میزان شکست یا موفقیت هر معیار در خروجی آزمایشگاه‌ها، محاسبه کرد. خروجی آزمایشگاه را می‌توان به صورت تعداد انجام درست تست‌ها به کل تست‌های آن سطح در خصوص هر معیار در نظر گرفت. به عنوان مثال در خصوص معیار مدیریت پارامترهای حساس ۸ مجموعه تست باید انجام شود (۱- مجموعه تست‌های مربوط به تولید عدد تصادفی، ۲- مجموعه تست‌های مربوط به تولید کلید، ۳- مجموعه تست‌های مربوط به توزیع کلید، ۴- مجموعه تست‌های مربوط به استقرار کلید، ۵- مجموعه تست‌های مربوط به ذخیره‌سازی کلید، ۶- مجموعه تست‌های مربوط به حفاظت از کلید، ۷- مجموعه تست‌های مربوط به امحای کلید و ۸- مجموعه تست‌های مربوط به ورود و خروج کلید). هر مجموعه تست از تعدادی تست تشکیل شده است اگر a_i به عنوان تست‌هایی که درست انجام شده در نظر گرفته شود نسبت a_i به A_i (که A_i کل تست‌های مجموعه iام است) عددی بین صفر و یک خواهد بود، میانگین مجموع این اعداد به صورت $\frac{\sum_{i=۱}^{۸} A_i}{۸}$ به عنوان خروجی آزمایشگاه برای معیار مدیریت پارامتر حساس است. متناسب با هر معیار دیگر در سطح دوم به همین صورت خروجی آزمایشگاه‌ها محاسبه کرد و حالت کلی معادله‌ی ترکیب خطی وزن‌دار این سطح به صورت زیر تشکیل می‌شود:

$$C = \sum_{j=۱}^{۵} b_j \frac{\sum_{i=۱}^{k_j} A_{ij}}{k_j} \qquad (۱)$$

در معادله فوق b_j ضریب ترکیب خطی و همان وزن فازی محاسبه شده برای معیار jام و A_{ij} کل مجموعه تست‌های iام از معیار jام است. همچنین k_j تعداد مجموعه تست یا به عبارتی تعداد زیرمعیارهایی است که درباره معیار jام در شکل ۶ ترسیم شده است. به عنوان مثال در خصوص معیار پارامترهای حساس تعداد این مجموعه تست همانطور که اشاره شد برابر با تعداد زیرمعیارها یعنی ۸ تا است.

از این‌رو میزان انطباق (C) که برای سطح ۲ می‌توان محاسبه کرد به صورت معادله زیر است:

$$C = ۰٫۳۶\frac{\sum_{i=۱}^{۸} A_{i۱}}{۸} + ۰٫۳۹\frac{\sum_{i=۱}^{۶} A_{i۲}}{۶} + ۰٫۱۹\frac{\sum_{i=۱}^{۶} A_{i۳}}{۶} + ۰٫۰۳\frac{\sum_{i=۱}^{۷} A_{i۴}}{۷} + ۰٫۰۳\frac{\sum_{i=۱}^{۷} A_{i۵}}{۷} \qquad (۲)$$

به همین صورت می‌توان برای سطح ۳ (سطح زیرمعیارها) انطباق را محاسبه کرد با این فرض که خروجی حاصل از هر معیار که برابر عبارت زیر است:

$$C^{(j)} = b_j \frac{\sum_{i=۱}^{k_j} A_{ij}}{k_j} \qquad (۳)$$

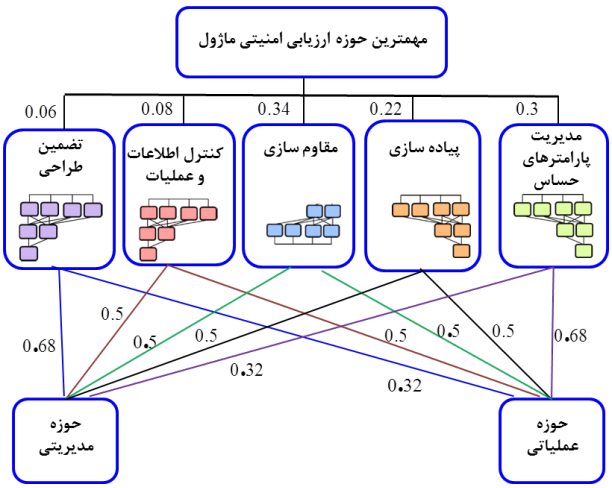
و این خروجی باید در وزن فازی مربوطه در سطح سوم ضرب شود تا در نهایت معادله ترکیب خطی وزن‌دار–فازی برای انطباق کل (C_T) محاسبه گردد:

$$C_T = \sum_{i=۱}^{۲}\sum_{j=۱}^{۵} c_{ij} C^{(j)} \qquad (۴)$$

که در عبارت بالا C_{ij} وزن مربوط از معیار jام در زیرمعیار iام است.

با توجه به اینکه در این روش از پرسشنامه جهت جمع‌آوری نظر کارشناسان خبره برای تعیین درجه اهمیت معیارها و زیرمعیارها استفاده شده است و متناسب با هر نظر کارشناسی می‌بایست وزن معیارها و زیرمعیارها استخراج گردد از این‌رو با روش‌های استدلالی، می‌توان به صورت استقرایی وزن بهینه را انتخاب کرد. اما در سال ۲۰۰۶ با استفاده از ادغام ماتریس‌های مقایسه‌ای حاصل از نظر کارشناسان این استدلال، دقیق‌تر شد و حجم محاسبات ماتریس‌های مقایسه دوتایی کاهش یافت [۲۳، ۲۴]. در نتیجه‌ی این ادغام، یک ماتریسی حاصل می‌شود که

[۱] مقدار هر یک از اوزان مذکور، بر مجموع کل آنها تقسیم می‌شود تا مجموع وزن‌های مربوط به کلیه معیارها معادل یک باشد.



شکل ۷. نمودار سلسله مراتب و وزن‌دهی معیارها و زیرمعیارها با روش ادغام نظر کارشناسان

درایه‌های آن را اعداد فازی مثلثی تشکیل می‌دهند و عناصر این اعداد فازی مثلثی به ترتیب کمترین مقدار، میانگین و بیشترین مقدار درایه‌ی متناظر آن در ماتریس‌های مقایسه دوتایی مربوط به هر کارشناس است. به عنوان مثال وزن‌های استخراجی بر اساس روش ادغام ماتریس‌های مقایسه دوتایی به صورت شکل ۷ تغییر پیدا کرده است.

۸ چالش‌های ارزیابی بومی ماژول رمز نگاشتی

به دلیل سیاست‌هایی که در ارزیابی بومی قائل خواهیم بود، برخی از چالش‌ها ممکن است مصداقی در فرآیندهای ارزیابی در جهان وجود نداشته باشد؛ مانند نوسانات قیمت در فرآیند ارزیابی، عدم وجود برآوردی درست از مدت زمان لازم برای ارزیابی همچنین و به دلیل تحریم‌ها می‌توان به چالش تهیه برخی تجهیزات به روز برای بررسی الزامات امنیتی یک محصول اشاره کرد. همان‌طور که در شکل ۸ نشان داده شده است پنج حوزه‌ی کلی شامل مردم، حاکمیت، نظارت، مقاوم‌سازی و مدیریت پردازش و زیربخش‌های آن‌ها به عنوان چالش‌های مطرح در فرآیند ارزیابی در نشان داده شده است که در ذیل همه‌ی آن‌ها چالش اساسی عدم وجود استاندارد و دستورالعمل بومی در ساختار ارزیابی قرار می‌گیرد. بنابراین هرگونه اقدام عمده در خصوص رفع این چالش‌ها باید با توجه به پیش‌نیاز تدوین استاندارد یا دستورالمعل بومی انجام گیرد.

۹ نتیجه‌گیری

در سال‌های اخیر رشد روزافزون فناوری اطلاعات و ارتباطات در جهات مختلف باعث به وجود آمدن مخاطراتی در حوزه‌های مختلف از جمله حوزه امنیت و ارزیابی امنیتی شده است. در این راستا انجام نظارت بر فرآیند ارزیابی و ایجاد اطمینان از صحت نتایج و روال‌ها در سطوح مختلف امنیتی به منظور صیانت از سرمایه‌های اطلاعاتی کشور با صدور مجوز فعالیت برای یک محصول در این حوزه (به عنوان مثال ماژول‌های رمزنگاشتی) از اهمیت بسزایی برخوردار است. از این‌رو استفاده از روش‌های مختلف تصمیم‌گیری چندمعیاره و تدوین معیارهای مناسب با بهره‌گیری از استانداردهای مرتبط در افزایش میزان دقت در اندازه‌گیری درصد انطباق یک محصول می‌تواند راهگشا باشد. در این مقاله با به‌کارگیری مدل ترکیب خطی وزن‌دار- فازی مبتنی بر روش تحلیل سلسله مراتبی فازی و بر اساس نظر خبرگان به ارائه‌ی فرمولی برای اندازه‌گیری دقیق‌تر درصد انطباق در فرآیند ارزیابی امنیتی یک ماژول رمزنگاشتی آن پرداخته و همچنین در این مقاله، به معرفی برخی چالش‌های ارزیابی بومی برای ماژول‌های رمزنگاشتی پرداخته شده است.

مراجع

[1] Security Requirements for Cryptographic Modules. Standard, NIST FIPS PUB 140-2, May 25 2001.

[2] Security Requirements for Cryptographic Modules. Standard, NIST FIPS PUB 140-3(Revised Draft), November 2009.

[3] Information technology- Security techniques, Evaluation Criteria for IT Security. Standard, ISO/IEC 15408, 2009.

[4] Common criteria. https://www.commoncriteriaportal.org. [Online] Available.

[5] Common criteria. https://www.niap-ccevs.org/Ref/CCRA.Partners.cfm. [Online] Available.

[6] Information technology- Security techniques. Standard, ISO/IEC 19790, 2012.

[7] Information technology- Security techniques. Standard, ISO/IEC 24759, 2017.

[8] PKCS. http://www.rsasecurity.com/rsalabs/pkcs. [Online] Available.

[9] ANSI X9. https://x9.org/standards/standards-store. [Online] Available.

[10] IETF. https://www.ietf.org/standards. [Online] Available.

[11] PKCS#11. https://docs.oasis-open.org/pkcs11/pkcs11-profiles/v3.0/pkcs11-profiles-v3.0.html. [Online] Available.

[12] Chang, Da-Yong. Applications of the extent analysis method on fuzzy ahp. *European journal of operational research*, 95(3):649–655, 1996.

[13] Yang, Ching-Chow and Chen, Bai-Sheng. Key quality performance evaluation using fuzzy ahp. *Journal of the Chinese Institute of Industrial Engineers*, 21(6):543–550,

شکل ۸. چالش‌های ارزیابی بومی

art survey & testbed of fuzzy ahp (fahp) applications. *Expert Systems with Applications*, 65:398–422, 2016.

[20] Zadeh, L. Fuzzy sets. *Inform Control*, 8:338–353, 1965.

[21] Yeh, Chi-Tsuen. Existence of interval, triangular, and trapezoidal approximations of fuzzy numbers under a general condition. *Fuzzy Sets and Systems*, 310:1–13, 2017.

[22] Saaty, Thomas L, Vargas, Luis G, et al. *Decision making with the analytic network process*, vol. 282. Springer, 2006.

[23] Chen, Ching-Fu. Applying the analytical hierarchy process (ahp) approach to convention site selection. *Journal of travel research*, 45(2):167–174, 2006.

[24] Chai, Junyi, Liu, James NK, and Ngai, Eric WT. Application of decision-making techniques in supplier selection: A systematic review of literature. *Expert systems with applications*, 40(10):3872–3885, 2013.

[25] Forman, Ernest H and Gass, Saul I. The analytic hierarchy process—an exposition. *Operations research*, 49(4):469–486, 2001.

2004.

[14] Lin, Hsiu-Fen. An application of fuzzy ahp for evaluating course website quality. *Computers & Education*, 54(4):877–888, 2010.

[15] Behzadian, Majid, Otaghsara, S Khanmohammadi, Yazdani, Morteza, and Ignatius, Joshua. A state-of the-art survey of topsis applications. *Expert Systems with applications*, 39(17):13051–13069, 2012.

[16] Figueiredo, Ciro and Mota, Caroline. Learning preferences in a spatial multiple criteria decision approach: An application in public security planning. *International Journal of Information Technology & Decision Making*, 18(04):1403–1432, 2019.

[17] Saaty, Thomas L. *Decision making for leaders: the analytic hierarchy process for decisions in a complex world*. RWS publications, 2001.

[18] Saaty, Thomas L and Peniwati, Kirti. *Group decision making: drawing out and reconciling differences*. RWS publications, 2013.

[19] Kubler, Sylvain, Robert, Jérémy, Derigent, William, Voisin, Alexandre, and Le Traon, Yves. A state-of the-

MonadiAfta-Bianual Scientific Journal for Cyberspace Security
2023, Volume 21, Number 1 (pp. 1–11)
https://monadi.isc.org.ir

On the Use of Fuzzy-WLC modeling technique for Evaluating Security of Cryptographic Module

Zahra Ferdosi [1] and Marjan Bahrololum [*,2]

[1] *Amirkabir University of Technology, Tehran, Iran*
[2] *Iran Telecommunication Research Center (ITRC), Tehran, Iran*

ARTICLE INFO.

Article history:
Received: April 3, 2022
Accepted: June 6, 2023
Published Online: July 8, 2023

Keywords:
Cryptographic Module
Evaluation Criteria
Fuzzy Hierarchical Analysis Process (FAHP)
Weighted Linear Combination Model (WLC model)

Type: Review paper

ABSTRACT

Development of information and communication technology has led to the increasing production of new products. One of the critical products that protect informational assets at various levels of security is the cryptographic module. Evaluating the security of cryptographic modules is critical for providing a reasonable degree of protection against attacks. Therefore, the security evaluation of a cryptographic module requires a strong awareness of the potential weaknesses that would become security flaws and careful consideration of security during all aspects of the evaluation process. In this paper, we present a comprehensive picture of the security evaluation criteria of the cryptographic module under existing international standards (e.g., FIPS 140-2 ,3 and ISO 15408, PKCS#11). In order to measure the compliance of these criteria correctly, we propose the model based on fuzzy-weighted linear combination. Also, the structure of any kind of evaluation requires considerable cost and time, which on the one hand, depends on the policies and requirements of the country, on the other hand depends on the facilities and experts. Finally, introducing and providing solutions that help solve the challenges, so we present some challenges about security evaluation in our country confirms the importance of study and research in this area.

* Corresponding author
Email addresses: ferdosi@aut.ac.ir (Zahra Ferdosi), bahrololum@itrc.ac.ir (Marjan Bahrololum)