تبیین امنیت فرآیندهای کتابخانه زیرساخت فناوری اطلاعات در اینترنت اشیاء با شبیه‌سازی فرآیندها

اکرم قنائی[۱]، محمدرضا ثنائی[۲،*]، جواد محرابی[۳]

[۱] دانشجوی دکتری، گروه مدیریت فناوری اطلاعات، واحد قزوین، دانشگاه آزاد اسلامی قزوین، ایران.

[۲] استادیار، گروه مدیریت فناوری اطلاعات، واحد قزوین، دانشگاه آزاد اسلامی، قزوین، ایران.(عهده دار مکاتبات)

[۳] استادیار، گروه مدیریت دولتی، واحد قزوین، دانشگاه آزاد اسلامی، قزوین، ایران.

چکیده

فرایندها یک از پایه‌های اصلی کتابخانه زیرساخت فناوری اطلاعات هستند که تامین امنیت آن‌ها برای پشتیبانی موثر از اهداف ضروری است. همچنین پیشرفت سریع اینترنت اشیاء در تمامی زمینه‌ها امکان گسترش آنرا فراهم کرده است. تحلیل و تامین برنامه‌های نوآورانه و ارائه راه‌حل‌های هوشمندانه جهت بالا بردن کیفیت تامین امنیت از طریق هماهنگ کردن اهداف با وضعیت روز و اصلاح و بهبود آن‌ها یکی از ارکان این تحقیق هستند. تجزیه و تحلیل روابط یکی از عوامل مهم برای امنیت فرآیندها است تا بدین وسیله بتواند نیازمندی‌های امنیتی IoT، ITIL، ابزارها، مدل‌ها و روش‌ها را برآورده کند. چهار حوزه و سه فاز امنیت عمومی، اختصاصی و انتشار در سه دسته آزاد، دانشگاهی و سازمانی با سناریوهای حمله، سطوح، احتمال رخداد حملات، پارامترها، معادلات و نرخ جریان در نظر گرفته شده که در مدل شبیه سازی ارائه شده است. آزمایش تغییر پارامتر مدل شبیه سازی و مدل‌های دستی را تحلیل و تایید می‌کند. در مرحله بعد، آزمایش کالیبراسیون برای تطبیق پارامترها با مقادیر خروجی انجام می‌گردد و مقادیر بهینه با توجه به تغییرات احتمالی در مدل شبیه سازی گنجانده می‌شوند.

واژه‌های اصلی: اینترنت اشیاء، کتابخانه زیرساخت فناوری اطلاعات، مدیریت فرایندها، مدل شبیه سازی

۱- مقدمه

امنیت فرایندها با توجه به محرک‌های موجود در اینترنت اشیاء نیاز به طرح و ارائه راه حل‌های هوشمندانه برای پیشبرد اهداف و جلوگیری از آسیب‌پذیری‌ها دارد. IoT از تجمع طیف وسیعی از داده‌های متصل به اینترنت تشکیل شده است در نتیجه با انجام خدمات جدید خطرات امنیتی افزایش می‌یابند[۱۳]. بدون شک موجودیت‌های مشترک(اشیاء) در IoT زمینه‌ای برای ایفای یک نقش فعال در فرایندها، سیستم‌ها و فعالیت‌های انسانی هستند[۳۷]. در کنار توسعه IoT حملات امنیتی روز به روز به تعداد آن افزوده می‌شود، بنابراین به یک مکانیسم دفاعی برای شناسایی و مقابله با حملات و تهدیدات در IoT نیاز است [۳۲]. مدیریت از موارد مهم است که در انجام تمامی مراحل تحقیق ارتباط بین دو فاکتور مورد نظر را ایجاد و از آن به شیوه‌های نوینی حمایت می‌کند. یکی از کارهای مدیریت این است که با کاهش و به حداقل رساندن مسیرهای حمله و پیچیدگی آن‌ها، هزینه حفاظت را به کمترین سطح ممکن برساند و بدین ترتیب سطوح امنیتی را به بالاترین سطح ممکن افزایش دهد که این مهم با تجزیه و تحلیل درست امکان‌پذیر می‌شود [۴۶]. موارد امنیتی را می‌توان با ابزارها، مدل‌ها، معیارها و همچنین روش‌ها مورد بررسی قرار داد، همچنین در می‌یابیم که افزایش امنیت زمان تاخیر را به طور چشمگیری کاهش می‌دهد که اغلب با صرف هزینه‌هایی می‌توان تاخیر را کاهش داد[۳۰, ۴۴]. با تجزیه و تحلیل دو مرحله‌ای فرآیندها و افرادی که در نوآوری شرکت دارند، بیشترین تاثیر در استراتژی تعیین می‌شود و بصورت سیستماتیک پیش‌بینی عملکرد فرآیندهای تازه طراحی شده انجام می‌شود[۱۲]. سیستم‌های امنیتی اطلاعات فرایندها را نیز شامل می‌شوند[۷] که لازم است امنیت آن‌ها تامین شوند. به تبع آن انباشت‌ها و جریان‌هایی که بر سیستم اثر می‌گذارند شناسایی و مورد توجه قرار می‌گیرند[۳۰] که در پی آن گزینه‌ها و فاکتورهای متعددی نیاز به تحلیل و بازنگری دارند.

* Mohamadrezasanaei@gmail.com

از همین منظر رز و همکاران[1] یک رویکرد مبتنی بر شبیه سازی ارائه دادند. این رویکرد انتخاب فرایندهای بهینه‌ای است که با در نظر گرفتن استراتژی‌ها می‌تواند به مدیران IT برای افزایش کارایی کمک کند. آن‌ها راه‌حل‌های بهینه را با استفاده از شبیه سازی ارائه دادند و نشان دادند چگونه این رویکرد می‌تواند به مدیران IT برای ارائه راه‌حل‌های با کیفیت کمک کند. آن‌ها نشان دادند راه حل‌های بهینه با استفاده از مدیریت تغییر نیاز به بهینه سازی چندین هدف دارد[۳۵]. در بررسی امنیت ITIL ضرورت دارد که امنیت فرایندها تامین شود به عبارت دیگر از آنجایی که ITIL، مدل مرجع مبتنی بر فرایند است یکی از بیشترین عواملی که بر موفقیت ITIL نقش دارد مدیریت مناسب فرایندهاست [۲۸]. در مبحث امنیت IoT و ITIL مدیریت امری مهم و حیاتی است و در حقیقت چون پلی بین فرایندها و ساختار در راستای دستیابی به استراتژی ایفای نقش می‌کند. در مرحله اول بررسی وضعیت فرایندها و آسیب‌پذیری‌ها انجام می‌شود و اطلاعات پیرامون فرایندها و آسیب‌پذیری‌ها درمرحله دوم ورودی تجزیه و تحلیل هستند. در تعریف بیانیه‌ها و چشم اندازها و ماموریت‌ها پیاده سازی فرایندهای ITIL در گام سوم با عنوان تحلیل موقعیت یکی از کارهای مهم انجام مطالعات موردی است [۴]. برای تامین امنیت فرایندهای ITIL در IOT و رسیدن به یک سیستم یکپارچه امن لازم است که ارزیابی دقیق و کامل اطلاعات و فرایندها، طبقه‌بندی و مدیریت فرایندها انجام شود. بطوریکه بدانیم عوامل تعیین کننده امنیت هر کدام از فاکتورها، ترکیبی از فاکتورها و تحلیل آن‌ها کدامند و چگونه بهبود می‌یابند. بدین منظور ساختار و اقدامات مهم در اولویت قرار می‌گیرند تا مشکلات امنیتی حداقل شده و به حداکثر رشد امنیتی دست یابیم. هدف این تحقیق تامین امنیت فرآیندهای ITIL در محیط IoT با توجه به عوامل موثر و تهدیدات امنیتی با ارائه مدل شبیه‌سازی است. این مدل با نوآوری در تحلیل، ترکیب مدل‌های دستی و سیستماتیک با دو فاکتور مذکور در حالات مختلف و سناریوهای احتمالی ارائه شده است. بدین منظور سعی در ارائه راه‌حل‌هایی برای بالا بردن کیفیت از طریق تامین امنیت دارد. هدف اصلی این تحقیق ارائه تحلیل‌ها و مدل‌هایی است که مدیران را جهت تصمیم‌گیری‌های بهینه بدون ریسک، هزینه، زمان با مقایسه عملکردها یاری‌کند.

۲- مبانی نظری پیرامون امنیت IoT، ITIL، تحلیل و ترکیب دو فاکتور

هدف از تامین امنیت فرایندها ایجاد یک محیط ایمن برای فرایندهایی است که انجام می‌شوند و تحت الزامات و مشخصات از پیش تعیین شده‌ای انتظار داریم به موفقیت برسند. بسیاری از مطالعات پیرامون IoT بر تکنولوژی‌ها، ادغام فناوری‌های در حال ظهور، معماری‌ها و برنامه‌ها تمرکز دارند [۶]. اتصالات فراوان در IoT منجر به بروز چالش-های امنیتی بسیاری شده است، که دارای فرمول کلاسیک و راه حل خاصی برای مسائل و مشکلات نیستند [۳۷]. الزامات امنیتی IoT بخشی از امواج نوآوری IoT است و می‌توان گفت بزرگترین چالش‌های امنیتی در IoT مربوط به روابط، قابلیت تعامل و همکاری بین اجزاء و فرایندهای موجود در IoT است [۳۲]. برای تشخیص تهدید بودن وقایع از تجزیه و تحلیل استفاده می‌شود. با توجه به سطح تهدید برنامه‌ریزی-های مربوط انجام می‌شود و بدین ترتیب ساختار و اقدامات مهم در اولویت قرار می‌گیرد. سپس اقدامات متقابل انجام می‌شود و طرح مناسب برای سطح امنیت پیشنهاد و درجه آسیب‌پذیری سیستم مشخص خواهد شد [۸, ۳۴, ۴۶]. امنیت مشکل اعتبارسنجی فرآیندها را حل می‌کند و بدین طریق می‌توان یک راه حل امن برای امنیت IoT ارائه داد[۴۳]. همچنین در کنار توسعه IoT حملات امنیتی روز به روز به تعداد آن افزوده می‌شوند، بنابراین به یک مکانیسم دفاعی برای شناسایی و مقابله با حملات و تهدیدات در IoT نیاز است[۳۲]. در تحقیقات انجام شده پیرامون امنیت IOT با بهره بردن از تحلیل ریسک‌های امنیتی می‌توان به کنترل پایدار در IOT دست یافت. در این تحقیقات از سناریوهای چندگانه برای نشان دادن خطرات و در پی آن تشخیص سریع‌تر حملات بهره برده‌اند[۱۴, ۱۵, ۲۳, ۳۲, ۴۰]. در ادامه لازم است نوع حملات از لحاظ ماهیت رفتاری آن‌ها مورد بررسی قرار گیرند. این حملات از نظر ماهیت رفتاری به دو بخش حملات فعال و غیرفعال تقسیم بندی می‌شوند. حملات فعال شامل حملات مسیریابی در شبکه‌های حسگر[2]، سرویس‌های انکار[3]، جعل[4]، فقدان همکاری[5]، تغییر و تبدیل[6]، جعل هویت[7] و استراق سمع[8] است و حملات غیرفعال شامل نظارت و استراق سمع[9]، تجزیه و تحلیل ترافیک[10] و مخفی سازی

[1] Ruiz et al

[2] Routing Attacks in Sensor Networks
[3] Dos
[4] Fabrication
[5] Lack of cooperation
[6] Modification
[7] Impersonation
[8] Eavesdropping
[9] Monitor & Eavesdropping
[10] Traffic Analysis

حمله کننده[11] است[۹, ۲۵, ۲۷, ۲۹, ۴۲]. این تقسیم بندی، انواع و تعداد حملات در تعداد انشعابات حملات عمومی در شکل ۳ ارائه شده است. در این شکل تعداد انشعابات برگرفته از احتمال رخداد حملات است.

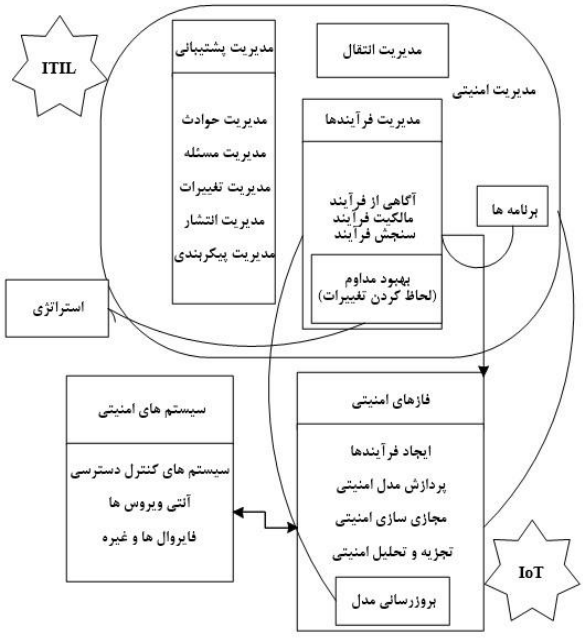
در ادامه تشریح فریندهای ITIL که تحت تاثیر محرک‌های IoT قرار دارند لازم است مبانی نظری پیرامون آن را از نظر بگذرانیم. مدیریت خدمت در IT بوسیله ارائه دهنده خدمت IT از طریق اختلاط مناسب افراد، فرآیندها و فناوری اطلاعات انجام می‌شود. مدیریت یک مبحث وسیع و دارای ابعاد مختلف است لذا یک مدیر برای انجام بهینه مدیریت نیازمند استفاده از فناوری‌های مختلف است. لازم است فناوری‌های مختلف با هم در ارتباط باشند و بصورت یکپارچه عمل کنند تا مدیریت عالی اتفاق بیفتد [۳۶]. معماری هسته ITIL بر پایه چرخه حیات خدمت است. هر دوره ITIL شامل راهبرد خدمت، طراحی خدمت، انتقال خدمت، عملیات خدمت و بهبود مداوم خدمات است که بر اهمیت هماهنگی و کنترل میان عملکردهای مختلف فرایندها و ملزومات سامانه‌ها برای مدیریت کامل چرخه حیات خدمات در IT تاکید دارد[۱, ۴]. همچنین فرآیندهای ITIL اطلاعات شامل: استراتژی، مدیریت کاتالوگ خدمت، مدیریت دانش، مدیریت حوادث و مدیریت درخواست است[۲, ۲۴]. برای مدیریت درست فرایندها و دستیابی به موفقیت می‌توان از شبیه‌سازی با مطالعه یک مورد استفاده کرد[۲۸]. ارتا و رز[12] روش جدیدی را برای چگونگی دستیابی به موفقیت با مدیریت درست فرایندها با استفاده از شبیه‌سازی و مطالعه یک مورد ارائه می‌دهند. این روش جدید کمک شایانی به مدیران در تصمیم‌گیری پیرامون فرآیندها و بهبود پیوسته آن‌ها ارائه می‌دهند[۲۸]. مدیریت امنیت تمام فرایندها را برای یافتن ریشه وقایع و اشکالات بکار می‌گیرد، روندها و بهبودها را در زمینه پایش نظاره کرده و همچنین در مورد این‌که استراتژی‌های امنیت نتایج دلخواه را فراهم نموده است مراقبت می‌کند[۳].

لازمه تامین امنیت فرایندهای ITIL در محیط IoT بررسی، شرح دو فاکتور مذکور، شناسایی عوامل حیاتی آنها، ارتباطات بین دو فاکتور، تشریح و تحلیل آن‌ها است. هر کدام از موارد موجود در دو فاکتور می‌تواند یک محرک برای فرایندها بوده و از لحاظ امنیتی فرایندها را دچار مشکل کند. لذا انجام تجزیه و تحلیل و شناسایی فرایندها، عوامل محرک آن‌ها و فاکتورها و روابطی که برای تامین امنیت نیاز است ضروری می‌نماید. از نظر کارشناسان مدیریت سیستم‌های تفکر تحلیلی بر اندیشیدن از خارج به داخل دلالت دارد، این درحالی است که تفکر ترکیبی بر اندیشیدن از داخل به خارج دلالت دارد و هیچ کدام ارزش دیگری را نفی نمی‌کند[۳۳]. ترکیب دو فاکتور IoT و ITIL تفکر داخل به خارج و تحلیل هر کدام از موارد نامبرده بر تفکر خارج به داخل اشاره دارد. با استقرار سیستم‌های IoT و افزایش آن‌ها امنیت یک جزء کلیدی برای حفاظت در دنیای فیزیکی و مجازی می‌شود[۳۸].

اکثر تحقیقات پیرامون امنیت IoT با تحلیل‌های کاربردی مدل‌های مختلف همراه است. در این تحقیقات به ضعف‌ها، حملات و توصیف چگونگی دسته‌بندی‌های مختلف امنیتی می‌پردازند. در برخی از این تحقیقات برای تامین و بهبود امنیت مدل شبیه‌سازی ارائه می‌شود[۱۱, ۱۸, ۲۰-۲۲, ۲۶, ۴۱, ۴۵]. در ادامه برای بررسی سطوح امنیتی با مشخص شدن وضعیت فرآیندها، گراف‌های حمله قابل تشخیص و بررسی است. استفاده از گراف‌های حمله یکی از راه‌های موثر برای مسائل IOT است[۱۰, ۱۷, ۱۹, ۳۸, ۳۹, ۴۳]. در تحقیقات بررسی شده پیرامون هر دو فاکتور شکاف‌های موجود، پارامترها و متغیرهای مورد بررسی در آن‌ها کنکاش می‌شود. بدین وسیله ارتباطات و سلسله مراتب امنیتی فرایندها در مدل‌های دستی ارائه می‌شود که این مدل-های دستی زمینه‌ای برای مدل شبیه‌سازی است. اولین قدم در تعیین ساختار، طراحی فرایند است[۳]. پشتیبانی فرآیندها از طریق مدیریت پشتیبانی با پنج فاکتور: مدیریت حادثه، مدیریت مسئله، مدیریت تغییر، مدیریت انتشار و مدیریت پیکربندی انجام می‌شود [۲۴]. به همین دلیل است که در پی ارتباطات و عواملی هستیم که بتواند فاکتورهای مرتبط را پوشش دهند. فرایندها از مهم‌ترین مواردی هستند که در اجرای موفقیت آمیز ITIL نقش دارند بطوریکه پولارد[13] و کاتر استیل[14] سه عامل برای موفقیت ITIL شناسایی کردند که یکی از مهم‌ترین آن‌ها اولویت دادن به فرایندهاست[۳۱]. توجه به این نکته ضروری است که اصول مدیریت فرایند شامل آگاهی از فرایند، مالکیت فرایند، سنجش فرایند و بهبود فرایند است[۲۸]. باید توجه کنیم با ITIL مدیریت و فرهنگ سازمانی تغییر می‌یابد این بدان معناست که در این راستا سعی در دستیابی به بهبود مستمر مدل با فرآیندها است[۴]. در این بین نقش اصلی استراتژی بروز رسانی لیست خدمات با خدمات جدید مرتب با کسب کار وهمچنین یافتن راه‌های توسعه سطوح خدمات و کاهش هزینه‌ها

[11] Camouflages Adversaries
[12] Orta & ruiz
[13] Pollard
[14] Cater-Steel

در ارائه این خدمات است و مسئولیت بروز رسانی و حفظ تمامی پیکربندی های برنامه را برعهده دارد[۳, ۵].



شکل۱. تشریح و انشعابات روابط امنیتی IoT و ITIL (مدل پایه دستی توضیحات ترکیبی)

به جهت این‌که قرار است امنیت را برای سیستم‌های IoT تامین کنیم، می‌توانیم در ابتدا یک مدل از سیستم IoT را به ظهور برسانیم. در ادامه نیازمندی‌های سیستم امنیتی و سطوح امنیتی را مشخص کنیم. سپس اجزاء، مکانیزم و آسیب‌پذیری‌های سیستم را بررسی و توصیف کنیم و یک مدل برای طراحی و اجرا ارائه دهیم[۱۶]. تکنولوژی امنیتی در IoT شامل سیستم‌ها و سرویس‌های امنیتی است. سرویس‌های امنیتی شامل سرویس‌های مشاوره، ارزیابی و عملیات سرویس هستند. سیستم-های امنیتی شامل سیستم‌های کنترل دسترسی، آنتی ویروس‌ها و فایروال‌ها هستند که شامل ایجاد محیط امن از طریق تحلیل‌های چندگانه و مدیریت مداوم برای امنیت سیستم‌های امنیتی است[۱۳]. پنج فاز برای تامین امنیت IoT پیشنهاد می‌شود: پردازش داده‌ها(ایجاد فرایند)، پردازش مدل امنیتی ، مجازی سازی امنیتی، تجزیه و تحلیل امنیتی، بروزرسانی مدل[۱۰]. ارائه مدل دستی شکل ۱ بر اساس مطالب ذکرشده ارتباطات بین اجزای مختلف دو فاکتور را نشان می-دهد.

۳- روش پژوهش

این تحقیق با تجزیه و تحلیل چندگانه و دو مرحله‌ای با مطالعه یک مورد در سه دسته آزاد، دانشگاهی و سازمانی در مدل شبیه‌سازی(نوعی آزمایش یا تجربه در محیطی همسان با محیط واقعی) ارائه شده است. به عبارت دیگر ساختار پایه در تحقیق برای ارائه مدل شبیه‌سازی شده از سه بخش تشکیل شده است: بخش اجرایی مدل، منطق مدل و توابع مدل. بخش اجرایی شبیه‌سازی شامل تجزیه و تحلیل دقیق و سازمان یافته عوامل مهم امنیتی دو فاکتور IoT و ITIL است. ترکیب و تحلیل دو فاکتور، گراف حملات، تعیین نواحی و ماژول‌های امنیتی در این بخش قرار دارند. در این قسمت اطمینان حاصل شد که تمامی عوامل موثر در شبیه‌سازی به درستی درگیر باشند. بخش دوم منطق مدل است که شامل معادلات، سطوح، نرخ جریانات و احتمال رخداد حملات است. این قسمت با بخش اجرایی در ارتباط است. بخش سوم توابع مدل است که شامل دسته‌های آزاد، دانشگاهی و سازمانی، مدل شبیه سازی، آزمایش تغییر پارامتر و آزمایش کالیبراسیون است. لازم به ذکر است که ابزار گردآوری اطلاعات و جداول، بانک‌های اطلاعاتی، شبکه‌های کامپیوتری، مشاهده و افراد متخصص در سازمان‌ها، ارگان‌ها و نهادها است.

٤- گراف حملات، ماژول‌های تحلیل امنیتی، مدل فشرده، مسیر حملات

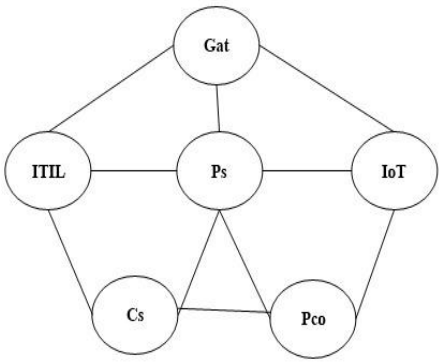
گراف حملات تمام توالی‌های ممکن برای اقدامات مهاجمان برای به مخاطره انداختن امنیت و اهداف آنان است. نشانه گذاری‌های مورد استفاده در گراف، اشکال و مسیرهای حملات در جدول ۱ ارائه شده است. تمام مجموعه مسیرهای حملات AP در گراف را نظر می-گیریم(شکل۲). برای یک هدف مشخص از سطح $ap \in AP$ دارای یک یا چند آسیب‌پذیری است. هر فرایندی که زیر مجموعه فرایندها است.P $p \in$ بنابراین:

$ap \in AP, AP \in Atg, P \in \{Gat, IoTs, ITILs, Ps, Cs, Pco\}$

جدول۱. معرفی و نشانه‌گذاری عناصر مورد استفاده

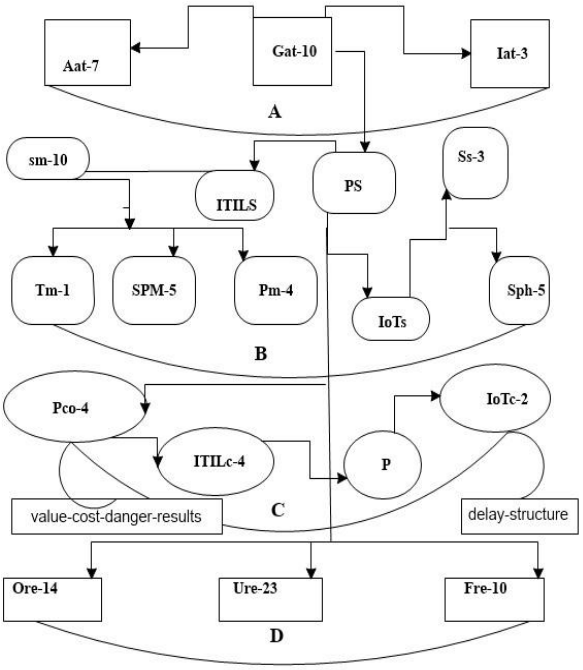
The elements used	Marking	The elements used	Marking	The elements used	Marking
General attacks	Gat	Active attacks	Aat	Conference	Co

IoT Security	IoTs	Passive attacks	Iat	Journal	Jo
Security system	Ss	Security phases	Sph	Processes	P
ITIL Security	ITILs	Free research	Fre	Total processes	Tp
Support management	Spm	IoT contents	IoTc	Case study time	Cst
Transfer management	Tm	Process management	Pm	Research time	Ret
Process contents	Pco	IoT contents	IoTc	Research	Re
Case study	Cs	Process security	Ps	Organizational research	Ore
Security management	Sm	Rate (*)	Each of the items used (*) r	The number of total researches	Tre
University research	Ure	Release cost	Rec	Total Security	Ts



شکل ۲. گراف حملات

این تحقیق شامل سه ماژول عمومی، اختصاصی، انتشار است . ماژول عمومی حملات سطوح مختلف و چگونگی تاثیر ارتباطات بر سایر ماژول‌ها است چرا که تمامی ماژول‌ها تحت تاثیر ماژول عمومی در محیط IoT و ITIL هستند(ناحیه امنیتی A و B و C). ماژول امنیتی اختصاصی در سه دسته آزاد، دانشگاهی و سازمانی مورد مطالعه مورد توجه قرار می‌گیرد(ناحیه امنیتی D).



شکل ۳. مدل فشرده شده دستی از نحوه ارتباط موارد تاثیرگذار بر ماژول‌ها

برای سه دسته مذکور حداکثر سطوح به عبارت ۱۴، ۲۳ و ۱۰ در نظر گرفته شده است. ماژول امنیتی انتشار (ژورنال و کنفرانس) مورد بررسی قرار می‌گیرند(ناحیه امنیتی D). حداکثر سطوح برای ژورنال و کنفرانس یه ترتیب ۲۴ و ۸ در نظر گرفته شده است. حملات عمومی تاثیر گذار بر تمامی ماژول‌ها در ناحیه امنیتی A، ارتباط بین فاکتورهای IoT و ITIL برگرفته از شکل ۳ ، محتوای فرآیندها در ناحیه امنیتی C و مطالعه موردی ناحیه امنیتی D(شکل ۴و۳). اعداد کنار هریک نمایانگر تعداد انشعابات است. بطور کلی هر فرایندی که زیر مجموعه فرآیندها است.$p \in P$ و AP مسیر حملات مشخص شده در گراف حمله بنابراین:

مسیرهای حملات ۱

$ap \in AP, AP \in Atg, PIOTs \in \{Re, (Ss,Sph), IoTsr\}$

$IoTs = (Re) \cap (Ss, Sph) \cap (IoTsr)$

$ap \in AP, AP \in Atg, PITILs \in \{P, (Tm,Spm,Pm), ITILsr\}$

ITILs = (P) ∩(Tm, Spm,Pm)∩(ITILsr)

ap∈Ap, AP∈Atg, P_{Cs}∈{Pco, (Cst,(Fre,Ure,Ore),Csc,Csr)}

Cs=(Pco)∩(Cst)∩(Fre, Ure,Ore)∩(Csr)∩(Csc)

ap∈AP, AP∈Atg, P_{Pco}∈{Ps, (ITILc, IoTc), Pcor}

Pco=(Ps)∩(IoTc, ITILc)∩(Pcor)

ap∈AP, AP∈Atg, P_{Ps}∈{Gat, (IoTs,ITILs), Psr}

Ps=(Gat) ∩(IoTs, ITILs) ∩(Psr)

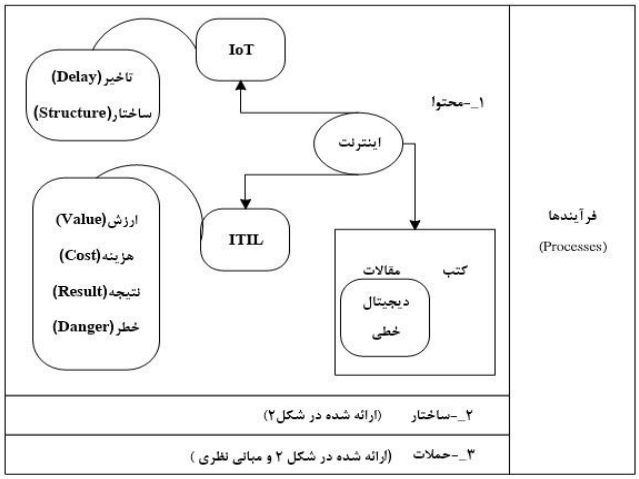
ap∈AP, AP∈Atg, P_{Gat}∈{(Aat, Iat),Gatr}

Gat=(Aat,Iat)∩(Gatr)

ap∈AP, AP∈ Atg, PTs∈{Cs, IoTs, ITILs, Jo,Co,Ret}

Ts = (Cs)∩ (IoTs)∩ (ITILs) ∩(Jo, Co) ∩ (Ret)

در این بین به دلیل این‌که از سیستم‌های پویا برای ارائه مدل شبیه سازی استفاده می‌شود لازم است یادآور شویم که تاخیرها از خصوصیات سیستم‌های پویا هستند که هر دو جریان مواد و اطلاعات را تحت تاثیر قرار می‌دهند. تاخیرها از هر نوعی که باشند می‌توانند تاثیر عمیقی بر سیستم بازخوردی داشته باشند[۳۰].



شکل ٤. تشریح ماژول امنیتی عمومی فرایندها

۴-۱ تشریح روابط و فرآیندها

اگر P_{SGPR} را مجموعه فرایندهای موجود در مدل SGPR بدانیم در آن-صورت روابط ۱ تا ۸ در فرآیندهای تحقیق و مدل شبیه‌سازی شده صادق است.

فرآیندهای هم راستا:

روابط و فرایندها ۱

$$\forall p1,p2 \in PSGPR,\ p1 \| p2$$

فرایندهای هم راستا به تشکیل فرایند بزرگتر کمک کرده و در صورت ایجاد امنیت هر کدام از فرایندهای هم راستا، امنیت فرآیند تشکیل شده تامین می‌گردد. فرایندهایی که برای تامین امنیت عمومی و اختصاصی ممکن است بطور همزمان و هم راستا اجرا شوند.

توالی فرآیندها:

روابط و فرایندها ۲

$$\forall p1,p2 \in PSGPR, p1,p2 \in= p$$

$$\forall p1,p2 \in P_{SGPR}, p1;p2 \Leftrightarrow end(p1) \leq start(p2)$$

توالی فرایندها، یک رابطه منظم دقیق بین دو فرایند که به صورت فوق نمایش داده می‌شود. . بدین معنی است که p1 قبل از p2 بطور کامل اجرا شده است. به عنوان مثال فرایند کامل انجام تحقیق بطور اختصاصی قبل از فرایند انتشار است و لازم است توالی فرایندها رعایت شود.

تعویض پذیری فرایندها:

روابط و فرایندها ۳

$$\forall p1,p2 \in PSGPR, p1,p2 \in= p2 \| p1$$

فرایندهایی که می‌توان برای تامین امنیت بطور موقت و یا دائم در هر دو محیط در جریان مدل‌سازی به صورت جایگزین از آن‌ها استفاده کرد. نتیجه در نهایت همان چیزی خواهد بود که انتظار انجام آن‌را داشتیم.

شرکت‌پذیری در فرایندها:

روابط و فرایندها ٤

$$\forall p1,p2,p3 \in PSGPR, (p1 \| p2) \| p3 = p1 \| (p2 \| p3) \in p$$

با توجه به موارد ذکر شده در فوق هر کدام از فرایندهایی که به نحوی اختلال در سیستم امنیتی را ایجاد کند می‌توان بر حسب ضرورت با توجه به روابط تعریف شده از فرایندهای جایگزین و یا ترکیبی از فرایندها استفاده کرد.

عملگر چرخه در فرایندها:

روابط و فرایندها ۵

$$LOOP(P)UNTIL\ C\ or\ LOOP(p,n)$$

اگر تعدادی از فرایندها در یک چرخه به تعداد n بار تکرار شود به صورت حلقه در مدل شبیه‌سازی نمایش داده می‌شود. در پاره‌ای از موارد ایجاد حلقه‌های بازخوردی در مدل ایجاد شده ضروری است. حلقه‌ها ممکن است بین دو یا چند فعالیت قرار گیرند این امر در انجام شبیه‌سازی به صورت حلقه‌های تقویتی و تعادلی هستند.

زمان و هزینه فرایندها:

A_{SGPR} را مجموعه فعالیت‌ها در مدل SGPR بدانیم و R^+ را مجموعه اعداد حقیقی مثبت فرض می‌کنیم. مدت زمان انجام یک فعالیت A به صورت زیر تعریف می‌شود:

روابط و فرایندها ۶

$$\forall A \in A_{SGPR}, duration(A) \in R^+$$

در مدل پویایی سیستم بازه زمانی (dt) از تفاضل آخرین نقطه زمانی تاکنون استفاده می‌شود.

روابط و فرایندها ۷

$$Dt=d_{max}-d_{min}$$

به عنوان مثال از این بازه زمانی در معادله سطح استفاده می‌شود:

روابط و فرایندها ۸

$$CL^{15}=PL^{16}+dt*(Ic^{17}-Oc^{18})$$

بنابراین، در نقطه زمانی فعلی، مقدار سطح یا انباره به سادگی برابر است با مقدار آن در نقطه زمانی پیشین بعلاوه خالص جریان‌های ورودی و خروجی در بازه (dt) که از آخرین نقطه زمانی تا کنون از سطح عبور کرده است.

۵- یافته‌های تحقیق

۵-۱ معیارهای سنجش

برای ارائه مدل شبیه سازی شده لازم است مواردی که در اجرای شبیه سازی نیاز است را محاسبه و مشخص نماییم. موارد یاد شده با توجه به ارتباطات، اشکال ارائه شده و مسیرهای حمله که پیشتر مشخص شده-اند ارائه می‌شوند. مراحل اجرای شبیه‌سازی سیستم‌های پویا برای مطالعه موردی در چهار بخش انجام می‌شود:

۱. تعیین معادلات
۲. تعیین احتمال رخداد حمله در هریک از سطوح و نرخ جریانات
۳. مشخص نمودن سطوح و نرخ جریانات
۴. ارائه مدل‌سازی سیستم پویا

۵-۲ معادلات

اگر برای شبیه‌سازی یک سیستم از پویایی سیستم استفاده شود، شناختن ماهیت معادله‌های نرخ امری حیاتی است. طریقه محاسبه و معادلات نرخ‌های جریان تاثیرگذار بر سطوح بدین ترتیب است:

نرخ های جریان تاثیرگذار ۱

(Gat)r=Aat*Iat
(ITILs)r=(Ms)r= Pm *Spm *Tm*P*Gatr/TP
(IoTs)r= Sph *Ss*Re*Gatr/TRE
(Ps)r= IoTs*ITILs (Sm)*Gat
(Pco)r= ITILc * IoTc*Ps
(Cs)r =Fre *Ure*Ore*Cst*Csc*Pco
(Ts)r=IoTs*ITILs*Jo*Co*Ret*Rec*Cs

۵-۳ احتمالات رخداد هریک از سطوح و نرخ جریانات

در این قسمت احتمال رخداد حملات حداکثری و حداقلی بر سطوح محاسبه گردید و احتمال رخداد حملاتی که نردیک به صفر بودند و قابل اغماض و چشم پوشی هستند، حذف شدند. احتمال رخداد حمله بر سطوح در جدول ۲ قابل مشاهده است.

جدول۲. پارامترها و مقادیر لحاظ شده در مدل شبیه سازی شده

[15] Current level
[16] Previous level
[17] Input currents
[18] Output currents

پارامترها= مقادیر				
Ss=0.37	Tm=0.1	Spm=0.5	IoTc=0.33	Ret=6
Pm=0.4	Sph=0.625	Fre=0.297	TRE=10000	Tp=20000
Ure=0.489	Ore=0.21	Aat=0.7	ITILc=0.66	Cst=24
Iat=0.3	Jo=0.041	Co=0.125	Rec=600	Csc=1500

۴-۵ مشخص نمودن سطوح و نرخ جریانات

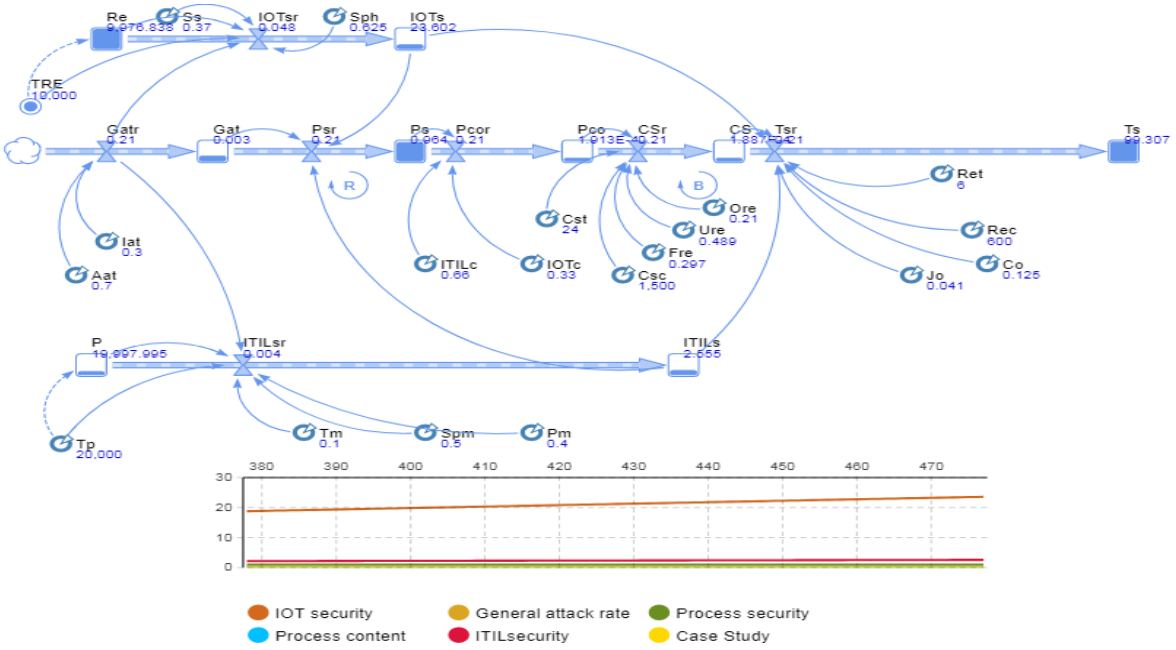
سطوح با نام‌های : Re، IoTs، Gat، Ps، Pco، Cs، Ts، P و ITILs.

جریانات با نام‌های : IoTsr، Gat، Psr، Pcor، Csr، Tsr، ITILsr.

پارامترها با نام‌های: *TRE*، *Ss*، *Sph*، *Aat*، *Iat*، *ITILc*، *IoTc*، *Cst*، *Fre*، *Ure*، *Ore*، *Jo*، *Co*، *Ret*، *Tp*، *Pm*، *Spm*، *Tm*، *Rec*، *Cst*.

۵-۵ ارائه مدل‌سازی سیستم‌های پویا

تمامی ارتباطات، معادلات و فرمول‌ها در قسمت‌های پیشین درج و بدان پرداخته شد. لوله‌های افقی جریان بین سطوح را نشان می‌دهد. تنها نقاطی که در آن‌ها می‌توان جریان سطوح را ایجاد کرد و یا از بین برد توسط ابرها نشان داده می‌شوند. از زمانی که یک جریان منبعی را ترک می‌کند تا زمانی که به سطح دیگری برسد تحت تاثیر قوانین بقا قرار دارد. پیکان‌های دیگر که به صورت خطی نمایش داده شده‌اند جریان اطلاعات هستند که قوانین بقا در مورد آن‌ها صدق نمی‌کند. سطوح به صورت مستطیل نمایش داده شده است که توسط جریان‌ها پر یا خالی می‌شوند. ما در این سیستم پویا قرار است وابستگی‌های علی را بررسی کنیم. و از دو نوع حلقه بازخورد می‌توانیم استفاده کنیم. با دور زدن حلقه در سیستم شبیه‌سازی درمی‌یابیم نیاز به حلقه به دلیل مغایرت با فرض اولیه همان‌طور که در *Cs* مشاهده می‌شود با افزایش امنیت فرایندها، امنیت در آن‌ها کاهش می‌یابد به همین دلیل از حلقه بازخوردی متعادل کننده استفاده می‌کنیم.



شکل ۵. اجرای شبیه‌سازی بعد از اضافه کردن حلقه‌ها و پالت زمانی

تعداد پیوندهای منفی ناموزون در *Cs* با کاهش *Gat* امنیت فرآیندها افزایش می‌یابد بنابراین نیاز به حلقه تقویت کننده داریم از یک حلقه تقویت کننده استفاده می‌کنیم. حلقه تقویت کننده را در *Psr* قرار می‌دهیم و سپس مدل را اجرا می‌کنیم. همان‌طور که در شکل ۵ ملاحظه می‌شود امنیت IoT(IoTs) در طول زمان افزایش می‌یابد، همچنین در طول زمان امنیت ITIL (ITILs) فزایش پیدا کرده هر چند میزان این افزایش کم است. در مورد حملات عمومی(Gat) که هدف ما کاهش مقدار آن است کاهش و مقدار صفر نزدیک می‌شود. در مورد حملات در

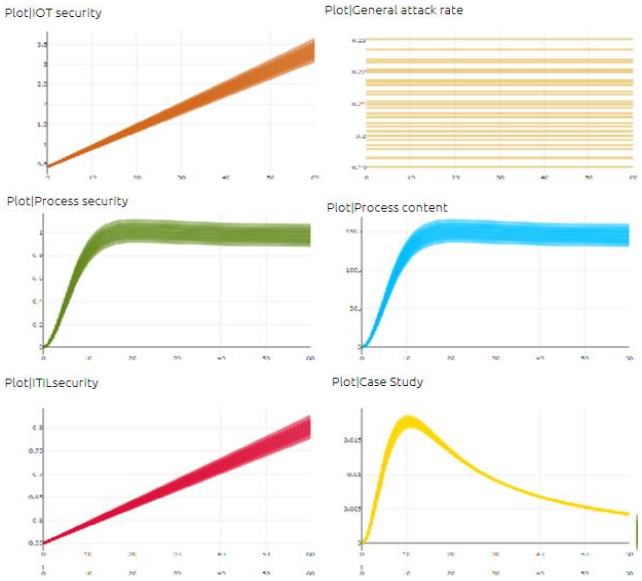
محتوای فرایندها(Pco) میزان بسیار کم(نزدیک به صفر) است و تقریبا در طول اجرا ثابت باقی می‌ماند. امنیت فرایندها(Ps) افزایش یافته، سپس مسیر ثابتی را ادامه می‌دهد و مطالعه موردی(Cs) تقریبا در همان میزان محاسبه شده باقی مانده و افزایش ناچیزی را دارد. در کل میزان افزایش امنیت IoT و امنیت ITIL محدوده قابل قبول و در حد انتظاری را به ما می‌دهد و در نهایت امنیت کل نیز افزایش می‌یابد.

۵-۶ آزمایش تغییر پارامتر

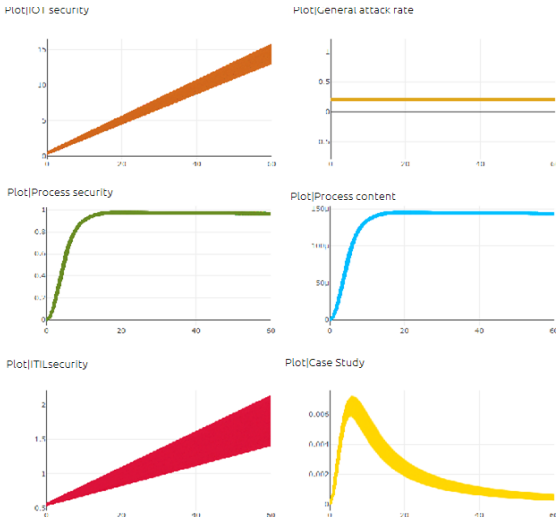
در این مرحله بوسیله Anylogic cloud به راحتی می‌توانیم آزمایش تغییر پارامتر را انجام دهیم. پس از اتمام آزمایش نتایج هر اجرا در یک نمودار نشان داده می‌شود تا به ما کمک کند درک بهتری از تاثیر پارامترهای مختلف بر نتایج داشته باشیم. به دلیل این‌که در این تحقیق تغییر عوامل و احتمال رخداد حمله مهم است بنابراین با تغییر احتمالات پارامترها نتایج را مشاهده خواهیم نمود. این آزمایش با تغییر محدوده پارامترها در نواحی امنیتی و برای مدیریت تغییر استفاده کاربردی دارد.

۱-۶-۵ متغیر نمودن و مشاهده نتایج فاز امنیتی عمومی، اختصاصی و انتشار

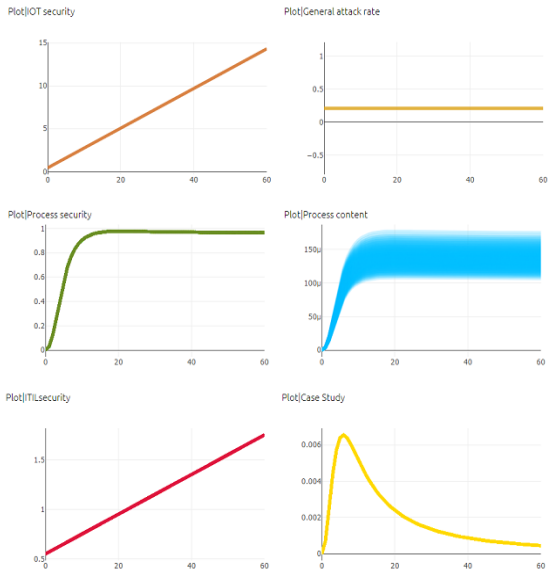
همان‌طور که در نمودارهای شکل ۶ مشاهده می‌شود تغییرات انجام شده در مرحله اول و پارامترهای حملات عمومی(Gat) تاثیر همه جانبه بر تمامی سطوح امنیت دارد. در مرحله دوم پارامترهای مربوط به IoTs و ITILs را متغیر نموده و نتایج را مشاهده می‌کنیم. چنان‌که که در نمودارهای شکل ۷ مشاهده می‌شود تغییر محدوده پنج پارامتر در مرحله دوم فاز امنیتی عمومی بررسی و مشاهده می‌شود. بدین ترتیب این تغییرات بر سه از سطح از سطوح مورد نظر تاثیرگذار است. این سه سطح عبارتند از امنیت IoT(IoTs)، امنیت ITIL(ITILs) و مطالعه موردی(Cs) است. بقیه موارد تقریبا بدون تغییر باقی می‌مانند. احتمال تغییر حمله، تغییر احتمال رخداد پارامترها را در پی دارد و در نهایت بر سه سطح مذکور در این فاز تاثیرگذار است. در نمودارهای شکل ۸ در مرحله سوم متغیر نمودن پارامترهای فاز امنیتی عمومی مشاهده می‌شود. تغییر محدوده پارامترها *Aat*، *IoTcIat* و *ITILc* ، بر تمامی فاکتورها تاثیرگذار است. همان‌گونه که در نمودارهای شکل ۹ مشاهده می‌شود تغییر محدوده پنج پارامتر هزینه مطالعه موردی(*Csc*)، مدت مطالعه موردی(*Cst*)، دسته آزاد(*Fre*)، دسته دانشگاهی(*Ure*)، دسته سازمانی(*Ore*) بر سطوح مختلف در فاز امنیتی اختصاصی مشاهده می‌شود. با اعمال تغییرات تمامی سطوح بجز محتوای فرآیندها(Pco) تقریبا بدون تغییر باقی می‌مانند. در فاز امنیتی انتشار با توجه به شکل بعد از تغییر محدوده چهار پارامتر هزینه مطالعه موردی(*Rec*)، انتشار مدت تحقیق(*Ret*) ژورنال(*Jo*) کنفرانس(*Co*) بیشترین تغییر در مطالعه موردی(Casestudy) مشاهده می‌شود. در بقیه موارد تقریبا تغییری مشاهده نمی‌شود. این تغییرات ابتدا افزایشی و سپس روند کاهشی را در پی داردکه در شکل ۱۰ قابل مشاهده است. در این مرحله و با توجه به شکل ۱۱ بعد از تغییر محدوده پارامترهای زمان و هزینه، شامل مدت انتشار(Ret)، مدت مطالعه موردی(Cst)، هزینه انتشار(Rec) و هزینه مطالعه موردی(Csc)در دو فاز امنیتی اختصاصی و انتشار بیشترین تاثیر در محتوای فرایندها(Pco) مشاهده می‌شود. همچنین در مطالعه موردی(Cs) همان‌طور که مشاهده می‌شود نیز به میزان کمی تاثیرگذار است. در بقیه موارد تقریبا تغییری مشاهده نمی‌شود.



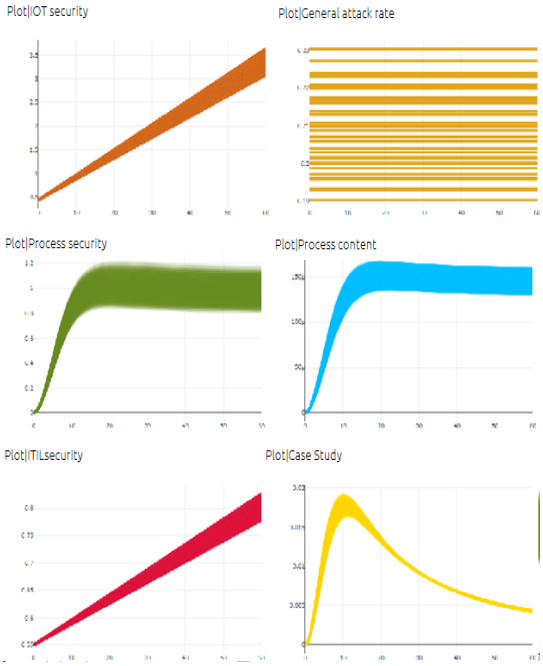
شکل ٦. مشاهده نتایج بعد از متغیر نمودن پارامترهای فاز امنیتی عمومی مرحله اول



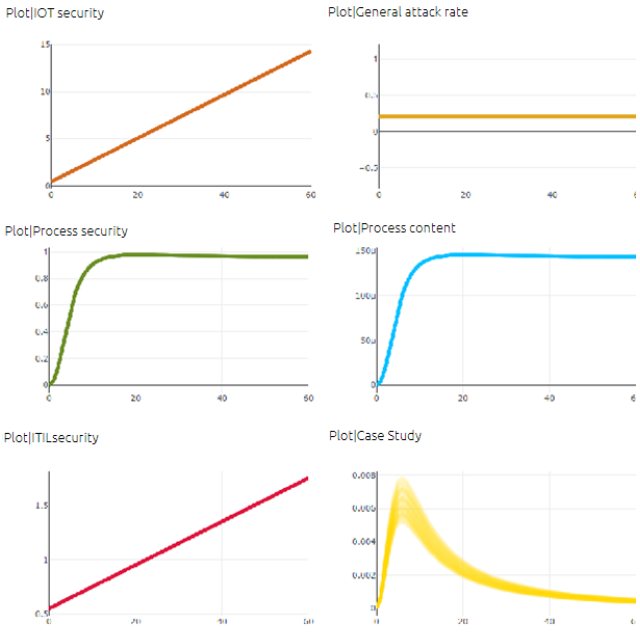
شکل ۷. مشاهده نتایج بعد از متغیر نمودن پارامترهای فاز امنیتی عمومی مرحله دوم



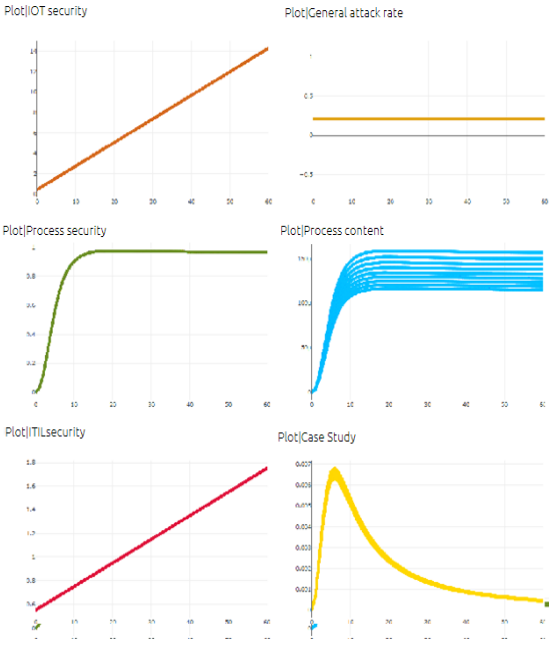
شکل ۹. مشاهده خروجی بعد از تعیین محدوده تغییر پارامترهای فاز اختصاصی



شکل۸. **مشاهده خروجی بعد از متغیر نمودن محدوده پارامترها فاز امنیتی عمومی مرحله سوم**



شکل ۱۰. مشاهده خروجی بعد از تعیین محدوده پارامترهای فاز امنیتی انتشار



شکل ۱۱. ***مشاهده خروجی بعد از تغییر محدوده پارمترهای زمان و هزینه***

٦- آزمایش کالیبراسیون

با ترکیب دو فاکتور و عوامل بصورت مدل‌های دستی و سیستماتیک شبیه‌سازی شده نیاز است تا با میزانی صحت و بهینه بودن آن اندازه-گیری شود. بدین ترتیب مقادیری را که بیشترین مطابقت را با مدل شبیه‌سازی و همچنین تناسب با داده‌ها دارند جایگزین می‌کنیم. با استفاده از ماکزیمم و مینیمم سازی از طریق چندین تابع هدف به بهترین سناریو برای مدل پیشنهادی دست می‌یابیم. آزمایش کالیبراسیون به صورت تکراری مدل را اجرا می‌کند، خروجی مدل را با داده‌های تاریخی مقایسه می‌کند و سپس مقادیر پارامتر را تغییر می-دهد. بعد از انجام یکسری آزمایش مشخص می‌شود که مقادیر کدام پارامترها با نتایج و الگوی تاریخی مطابقت بیشتری دارد. آزمایش کالیبراسیون را برای سه فاز عمومی، اختصاصی و انتشار و همچنین هزینه و زمان بطور جداگانه انجام می‌دهیم. یک پایگاه داده با نام "TsDS" (Ts data set) ایجاد می‌کنیم و داده‌های تاریخی را با ایجاد یک تابع جدولی با نام TsHistory ذخیره می‌کنیم. که با فراخوانی تابع مقداری را به آرگومان تابع منتقل و یک مقدار تابع را برمی‌گرداند. این آزمایش را در چهار مرحله عمومی، اختصاصی، انتشار و زمان و هزینه با تغییر پارامترهایی که در ساختار فرآیندها مهم هستند انجام می‌دهیم. پنج پارامتر از فاز عمومی امنیت سیستم(Ss)، فازهای امنیتی(Sph)، مدیریت انتقال(Tm)، مدیریت فرآیندها(Pm)و مدیریت پشتیبانی(Spm)، سه پارامتر از فاز اختصاصی دسته‌های آزاد(Fre)، دانشگاهی(Ure) و سازمانی(Ore) و دو پارامتر از فاز انتشار ژورنال(Jo) و کنفرانس(Co) و مدت انتشار(Ret)، هزینه انتشار(Rec)، مدت مطالعه موردی(Cst) و هزینه مطالعه موردی(Cs) در بخش زمان و هزینه در آزمایش کالیبراسیون در سه فاز نامبرده را از حالت Fixed به حالت Continuous تغییر می‌دهیم. اطلاعات مورد نیاز برای اجرای دستور کالیبراسیون را در جعبه‌ها قرار داده و آزمایش را اجرا می‌کنیم. پس از انجام و کامل شده آزمایش کالیبراسیون می‌توانیم با کلیک بر روی بهترین گزینه بهترین مقدار پارامتر را کپی کرده و در آزمایش جایگذاری کرده و با مقادیر پارامتر جدید کالیبره شده اجرا می‌کنیم. بهترین مقادیر بدست آمده در شکل ۱۲ قابل مشاهده است.

Ss=0.4 Tm=0.12 Spm=0.52 Pm=0.42 Sph=0.65	بهترین گزینه های کالیبراسیون پارامترها در فاز عمومی
Fre=0.35 Ure=0.51 Ore=0.23	بهترین گزینه های کالیبراسیون پارامترها در فاز اختصاصی
Jo=0.043 Co=0.15 Ret=6.2 Cst=26	بهترین گزینه های کالیبراسیون پارامترها در فاز انتشار
Ret=6.2 Cst=30 Csc=2002 Rec=602	بهترین گزینه ها ی کالیبراسیون پارامترهای زمان و هزینه

شکل ۱۲. بهترین مقادیر پارمترها بعد از انجام آزمایش کالیبراسیون

۷- مقایسه، بحث و نتیجه گیری

در اکثر کارهای تحقیقاتی، روابط بین ریسک‌ها، تهدیدها و حملات با عناصر اصلی تحقیق به صورت متریک در نظر گرفته می شود. همچنین، این روابط فقط برای مطالعه موردی خاصی در نظر گرفته شده است. پژوهش حاضر به صورت دستی و با در نظر گرفتن احتمالات بین عناصر تأثیرگذار در هر یک از سطوح شبیه سازی شده است. این روابط و احتمالات بر اساس مطالعه موردی در سه دسته انجام شده است که بنا به ضرورت عناصر، روابط و احتمالات آن قابل تغییر، تنظیم، محاسبه و جایگزینی است. در نهایت روابط، احتمالات و شبیه‌سازی‌های پیشنهادی پتانسیل‌هایی را برای تحلیل بهتر و تصمیم‌گیری‌های مهم‌تر ایجاد می‌کنند. روند تبدیل داده‌های خام به نتایج بدین ترتیب است:

ابتدا تعداد انشعابات را با توجه به امنیت فرآیندها در دو فاکتور مذکور بدست می‌آوریم. سپس مقادیر احتمال حملات را با تجزیه و تحلیل روابط بین سطوح مختلف و با توجه به گراف حملات محاسبه می‌کنیم. در ادامه مقادیر نزدیک به صفر را حذف می‌کنیم و احتمالات و سطوح در مدل شبیه‌سازی لحاظ می‌نماییم. با آزمایش تغییر پارامتر مقادیر پارامترها را تغییر و جایگزین می‌کنیم تا میزان و نحوه تاثیر بر سطوح امنیتی مشخص گردد. همچنین احتمال حملات در مدل ارائه شده در هر کدام از فاکتورهای IOT و ITIL بطور جداگانه قابل تغییر و تاثیر آن بر سطوح هر کدام از فاکتورها و ترکیبی از دو فاکتور قابل مشاهده و انجام پذیر است. در آزمایش کالیبراسیون برای صحت اطمینان از درستی روابط و احتمالات در مدل‌های دستی و سیستماتیک انجام می‌شود. است. موارد ارائه شده در واقع پتانسیل‌های را برای تحلیل بهتر و تصمیم‌گیرهای مهم‌تر ارائه می‌کند. پیشنهادات در راستای تامین امنیت:

۱. بررسی دقیق‌تر و عمیق‌تر مسائل اقتصادی و زمانی در تامین امنیت و ارائه دستاوردهای پژوهشی. این بررسی بر تکمیل و محاسبه احتمال رخداد حمله و ارائه مدل شبیه‌سازی شده نتایج قابل توجهی را به دنبال خواهند داشت.
۲. بررسی کیفی و کمی آسیب‌ها و تهدیدات امنیتی
۳. کاهش درگاه‌های ارتباطی و سطوح
۴. عدم سرمایه‌گذاری امنیتی بر سطوح غیر ضروری به دلیل کوچک بودن عدد احتمال رخداد حمله
۵. بهره بردن از مدیریت تغییر در صورت استفاده از مدل‌های شبیه‌سازی پیرامون فرایندها جهت در نظر گرفتن تمامی جوانب مختلف

منابع و ماخذ :

[1] Axelos, ITIL4 foundation 2019: Axelos.
[2] Bayona, S., Y. Baca, and G. Vela. IT service management using ITIL v3: A case study. in 2017 12th Iberian Conference on Information Systems and Technologies (CISTI). 2017. IEEE.
[3] Bon, J.v., ITIL V3 - A Pocket Guide (Best Practice) Kindle Edition2007: Van Haren Publishing.
[4] CANNON.D, ITIL SERVICE STRATEGY2011, UNIVERSITY TEHRAN Publishers.
[5] Castillo, F., Managing Information Technology. illustrated ed2016: Springer.
[6] Chae, B.K., The evolution of the Internet of Things (IoT): A computational text analysis. Telecommunications Policy, 2019: p. 101848.
[7] Clinch, J., ITIL V3 and information security. Best Management Practice., 2009.
[8] Das, A.K., S. Zeadally, and D. He, Taxonomy and analysis of security protocols for Internet of Things. Future Generation Computer Systems, 2018. **89**: p. 110-125.
[9] Douceur, J.R. The sybil attack. in International workshop on peer-to-peer systems. 2002. Springer.
[10] Ge, M., et al., A framework for automating security analysis of the internet of things. Journal of Network and Computer Applications, 2017. **83**: p. 12-27.
[11] Guo, H., et al., A scalable and manageable IoT architecture based on transparent computing. Journal of Parallel and Distributed Computing, 2018. **118**: p. 5-13.
[12] Han, K.H., Kang, J. G., & Song, M., Two-stage process analysis using the process-based performance measurement framework and business process simulation. Expert Systems with Applications,, 2009. **36(3), 7080-7086.**
[13] Hong, S. and e. al, An analysis of security systems for electronic information for establishing secure internet of things environments: Focusing on research trends in the security field in South Korea. Future Generation Computer Systems, 2018. **82**: p. 769-782.
[14] Hossain, M., et al., An Internet of Things-based health prescription assistant and its security system design. Future Generation Computer Systems, 2018. **82**: p. 422-439.
[15] Huang, X., et al., SecIoT: a security framework for the Internet of Things. Security and communication networks, 2016. **9**(16): p. 3083-3094.
[16] Iden, J., Investigating process management in firms with quality systems: a multi-case study. Business Process Management Journal,, 2012. **18(1), 104-121.**
[17] Ingols, K., et al. Modeling modern network attacks and countermeasures using attack graphs. in 2009 Annual Computer Security Applications Conference. 2009. IEEE.
[18] Jang, J., I.Y. Jung, and J.H. Park, An effective handling of secure data stream in IoT. Applied Soft Computing, 2018. **68**: p. 811-820.
[19] Jiang, H., et al., A secure and scalable storage system for aggregate data in IoT. Future Generation Computer Systems, 2015. **49**: p. 133-141.
[20] Lee, Y., J. Jeong, and Y. Son, Design and implementation of the secure compiler and virtual machine for developing secure IoT services. Future Generation Computer Systems, 2017. **76**: p. 350-357.
[21] Lim, S., O. Kwon, and D.H. Lee, Technology convergence in the Internet of Things (IoT) startup ecosystem: A network analysis. Telematics and Informatics, 2018. **35**(7): p. 1887-1899.
[22] Madhusudhan, R., A secure and lightweight authentication scheme for roaming service in global mobile networks. Journal of information security and applications, 2018. **38**: p. 96-110.
[23] Mavropoulos, O., et al., Apparatus: A framework for security analysis in internet of things systems. Ad Hoc Networks, 2019. **92**: p. 101743.
[24] McNaughton, B., P. Ray, and L. Lewis, Designing an evaluation framework for IT service management. Information & Management, 2010. **47**(4): p. 219-225.
[25] Mitrokotsa, A., M.R. Rieback, and A.S. Tanenbaum, Classification of RFID attacks. Gen, 2010. **15693**: p. 14443.
[26] Moon, J., I.Y. Jung, and J.H. Park, Iot application protection against power analysis attack. Computers & Electrical Engineering, 2018. **67**: p. 566-578.
[27] Muhammad, M.F., W. Anjum, and K.S. Mazhar, A Critical Analysis on the Security Concerns of Internet of Things (IoT). International Journal of Computer Applications (0975 8887), 2015. **111**(7).
[28] Orta, E. and M. Ruiz, Met4ITIL: A process management and simulation-based method for implementing ITIL. Computer Standards & Interfaces, 2019. **61**: p. 1-19.
[29] Padmavathi, D.G. and M. Shanmugapriya, A survey of attacks, security mechanisms and challenges in wireless sensor networks. arXiv preprint arXiv:0909.0576, 2009.

[30] pidd, M., Computer simulation in management science and industrial engineering, ed. 42016: Wiley; sharif.
[31] Pollard, C. and A. Cater-Steel, Justifications, strategies, and critical success factors in successful ITIL implementations in US and Australian companies: an exploratory study. Information systems management, 2009. **26**(2): p. 164-175.
[32] Rathore, S. and J.H. Park, Semi-supervised learning based distributed attack detection framework for IoT. Applied Soft Computing, 2018. **72**: p. 79-89.
[33] Rezaaian, A., Fundamentals Organization and management2015: Samt.
[34] Roy, A., D.S. Kim, and K.S. Trivedi, Attack countermeasure trees (ACT): towards unifying the constructs of attack and defense trees. Security and communication networks, 2012. **5**(8): p. 929-943.
[35] Ruiz, M., et al., Using simulation-based optimization in the context of IT service management change process. Decision Support Systems, 2018. **112**: p. 35-47.
[36] sadeghi, M. and a. hossaini, Information Technology management(Volume One - Management Strategy)2014: Mani publisher.
[37] Sfar, A.R., et al., A roadmap for security challenges in the Internet of Things. Digital Communications and Networks, 2018. **4**(2): p. 118-137.
[38] Sha, K., et al., On security challenges and open issues in Internet of Things. Future Generation Computer Systems, 2018. **83**: p. 326-337.
[39] Stergiou, C., et al., Secure integration of IoT and cloud computing. Future Generation Computer Systems, 2018. **78**: p. 964-975.
[40] Sun, P., et al., Modeling and clustering attacker activities in IoT through machine learning techniques. Information Sciences, 2019. **479**: p. 456-471.
[41] Tewari, A. and B. Gupta, Security, privacy and trust of different layers in Internet-of-Things (IoTs) framework. Future Generation Computer Systems, 2018.
[42] Thakur, B.S. and S. Chaudhary, Content sniffing attack detection in client and server side: A survey. International Journal of Advanced Computer Research, 2013. **3**(2): p. 7.
[43] Wang, K.-H., et al., A secure authentication scheme for Internet of Things. Pervasive and Mobile Computing, 2017. **42**: p. 15-26.
[44] White, G., V. Nallur, and S. Clarke, Quality of service approaches in IoT: A systematic mapping. Journal of Systems and Software, 2017. **132**: p. 186-203.
[45] Yang, J.-C. and B.-X. Fang, Security model and key technologies for the Internet of things. The Journal of China Universities of Posts and Telecommunications, 2011. **18**: p. 109-112.
[46] Yiğit, B., et al., Cost-aware securing of IoT systems using attack graphs. Ad Hoc Networks, 2019. **86**: p. 23-35.