چارچوبی برای امنیت فرایندهای کتابخانه زیرساخت فناوری اطلاعات در محیط اینترنت اشیا

اکرم قنائی

دانشجوی دکتری، گروه مدیریت فناوری اطلاعات، واحد قزوین، دانشگاه آزاد اسلامی، قزوین، ایران

محمدرضا ثنائی*[1]

استادیار، گروه مدیریت فناوری اطلاعات، واحد قزوین، دانشگاه آزاد اسلامی، قزوین، ایران

جواد محرابی

استادیار، گروه مدیریت دولتی، واحد قزوین، دانشگاه آزاد اسلامی، قزوین، ایران

مدیریت اطلاعات

دوره ۷، شماره ۲

پاییز و زمستان ۱۴۰۰

چکیده: امنیت فرایندهای کتابخانه زیرساخت فناوری اطلاعات با توجه به محرک‌های موجود در محیط اینترنت اشیا به راه‌کارهای هوشمندانه برای پیشبرد اهداف و جلوگیری از آسیب‌پذیری‌ها نیاز دارد. برای تأمین امنیت و به حداکثر رساندن سطوح امنیتی، به مدیریت مناسب نیاز است تا بتوان مسیرهای پیچیده را حذف کرد، عملکرد را بهبود بخشید، ساختار فرایندهای کتابخانه زیرساخت فناوری اطلاعات را بهینه و در نهایت، اهداف را در دسترس کرد. پژوهش حاضر بر اساس تجزیه‌وتحلیل دقیق روابط، مدل‌های دستی و سیستماتیک با بررسی امنیت دستاوردهای پژوهشی در سه دسته آزاد، دانشگاهی و سازمانی ارائه می‌شود. احتمال رخداد حملات در فرایندها در چهار ناحیه و سه ماژول عمومی، اختصاصی، انتشار با تحلیل سناریوهای امنیتی و با سطوح حداکثری در مدل شبیه‌سازی لحاظ می‌شوند. سطوح حداکثری در مطالعه موردی، ماژول امنیتی اختصاصی در دسته آزاد ۱۰، دسته دانشگاهی ۲۳، دسته سازمانی ۱۴ و در ماژول امنیتی انتشار، ۲۴ سطح برای ژورنال و ۸ سطح برای کنفرانس در نظر گرفته می‌شوند. در تعیین احتمال رخداد حملات، احتمالاتی که می‌توان از آنها چشم‌پوشی کرد و به صفر نزدیک هستند، حذف می‌شوند. بقیه موارد به انضمام معادلات، پارامترها، سطوح و جریان‌ها در مدل کلی لحاظ می‌شوند. در ادامه، بر پایه اطلاعات موجود، مدل شبیه‌سازی ارائه می‌شود، آزمایش‌های تغییر پارامتر و کالیبراسیون انجام شده و بهترین مقادیر ممکن متناسب با داده‌ها نیز مشخص می‌شوند. این پژوهش با ارائه مدل‌های دستی و سیستماتیک سعی در ایجاد امنیت با تخمین تأثیر حالات حدی در فرایندها به‌وسیله شبیه‌سازی دارد. همچنین بهینه‌سازی تغییرات احتمالی برای مدیریت تغییر را فراهم آورده (آزمایش تغییر پارامتر و کالیبراسیون) و مدیران را به اخذ تصمیم‌های بدون القای ریسک، هزینه و زمان با توجه به سناریوهای موجود قادر می‌کند.

کلیدواژه‌ها: IoT، ITIL، امنیت فرایندها، چارچوب، شبیه‌سازی.

---

۱. نویسنده مسئول: mohamadrezasanaei@gmail.com

مقدمه

تأمین امنیت فرایندهای کتابخانه زیرساخت فناوری اطلاعات (ITIL)[1] برای پشتیبانی مؤثر از اهداف ضروری است. همچنین پیشرفت سریع اینترنت اشیا (IoT)[2] در تمامی زمینه‌ها امکان گسترش آن را در تمامی زمینه‌ها فراهم کرده است. در IoT هر شیء فیزیکی در دنیای مجازی پذیرفته‌شده، در دسترس و تنظیم می‌شود (Roman, Zhou & Lopez, 2013; Ge, Hong, Guttmann & Kim, 2017; Sicari, Rizzardi, Grieco, & Coen-Porisini, 2015). فاکتور هوشمند از شخص، اشیای هوشمند، فرایندها و اکوسیستم تکنولوژیکی به‌عنوان عناصر اصلی رویکرد سیستماتیک ما برای امنیت IoT تشکیل شده است (Sfar, Natalizio, Challal & Chtourou, 2018). در دنیای امروز، از فرایندها و نوآوری‌های فرایندها برای پیشرفت و دستیابی به اهداف استفاده می‌شود (Han, Kang & Song, 2019). در کنار توسعه IoT حملات امنیتی، روزبه‌روز به تعداد آن افزوده می‌شود، بنابراین برای شناسایی و مقابله با حملات و تهدیدها در IoT به سازوکاری دفاعی نیاز است (Rathore & Park, 2018). بهبود اثربخشی از طریق فرایندها ، شیوه‌های مدیریتی، تأکید بر ساختار و تغییرات همه‌جانبه در سایه امنیت امکان‌پذیر است (French & Bell, 1995).

در ابتدا، برای ارائه سازوکار امنیتی فقط کار تجزیه‌وتحلیل اطلاعات انجام می‌شود. بدین ترتیب، ساختار و اقدامات مهم پیرامون فرایندها در اولویت قرار می‌گیرد، همچنین فرایندها که تأثیر بیشتری در استراتژی دارند، مشخص می‌شوند (Pidd, 2004; Han et al, 2019). موارد امنیتی را می‌توان با ابزارها، مدل‌ها، معیارها و همچنین روش‌ها بررسی کرد (White, Nallur & Clarke, 2017; Stergiou, Psannis, Kim & Gupta, 2018). با توجه به رشد تکنولوژی باید مشکلات امنیتی را به حداقل برسانیم تا بتوانیم با توسعه سریع به حداکثر رشد امنیتی دست پیدا کنیم (Stergiou et al, 2018).

از آنجا که ITIL، مدل مرجع مبتنی بر فرایند است، یکی از عواملی که بر موفقیت ITILنقش دارد، مدیریت مناسب فرایندهاست (Orta & Ruiz, 2019; Law, Kelton & Kelton, 2000). در مرحله نخست، بررسی وضعیت فرایندها و آسیب‌پذیری‌ها انجام می‌شود و اطلاعات پیرامون فرایندها و آسیب‌پذیری‌ها در مرحله دوم ورودی تجزیه‌وتحلیل هستند. در گام سوم، با عنوان تحلیل موقعیت یکی از کارهای مهم انجام مطالعات موردی است (Cannon, 2011). نخستین گام در تعیین ساختار، طراحی فرایندها است (Bon, 2011). در مدل‌بندی فرایندها باید طراحی فرایندها ، توسعه مدل، پیاده‌سازی، نظارت و ارزیابی انجام شود (Orta, Ruiz, Hurtado & Gawn, 2014). اکثر نهادها روی تمرکز بر فرایندها قبل از انتخاب، پیاده‌سازی، اجرا، پشتیبانی، تغییر و ادغام فرایندها ، اجماع و توافق دارند (Pollard, & Cater-Steel, 2009). راهکارها برای بهبود فرایند در سه فاز سازمان‌دهی می‌شوند. نخست تعیین زمینه، دامنه و اهداف فرایند، دوم درک فرایند موجود (مدل‌سازی جریان کار) و سوم طراحی فرایند جدید مطلوب (ارزیابی و انتخاب بهبودها) (Sharp & McDermott, 2009).

1. Information Technology Infrastructure Library
2. Internet of Thing

یک مطالعه موردی (تحلیل موقعیت)، با لحاظ کردن انگیزه‌های پیاده‌سازی مزایای پیاده‌سازی، وضعیت پیاده‌سازی و نتایج پیاده‌سازی، به‌همراه تمرکز داشتن روی مسائل واقعی فرایندها ، درک درست از تعریف فرایندها و تعیین گراف‌ها حمله در سطوح امنیتی، روند تکامل چارچوب نهایی را نشان می‌دهد (Ge et al, 2017; Ahmad, Amer, Qutaifan& Alhilali, 2013; Saini, Duan & Paruchuri, 2008; Ingols, Chu, Lippmann, Webster & Boyer, 2009;). شاید بتوان گفت که این پژوهش، نخستین رویکرد شبیه‌سازی سیستم‌های پویا برای تأمین و بهبود امنیت فرایندها با دو فاکتور IoT و ITIL به‌وسیله گراف امنیتی و احتمال رخداد حملات برای ارائه مدل شبیه‌سازی SGPR[1] است. در ادامه به این پرسش‌ها پاسخ می‌دهیم که در تأمین و بهبود امنیت IoT و ITIL چه عواملی تعیین‌کننده‌اند، تحلیل امنیتی پژوهش و ترکیب آنها چگونه انجام می‌شود و آیا می‌توان به چارچوب امنیتی ترکیبی پیرامون IoT و ITIL دست یافت؟

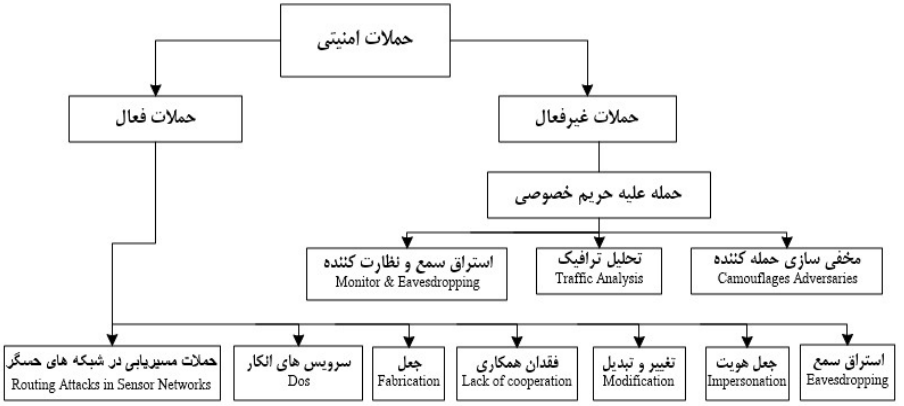
مبانی نظری پیرامون IoT و امنیت IoT

IoT سیستمی از اشیای فیزیکی و مجازی است که هر یک در قابلیت‌های شبکه گنجانده شده‌اند و برای تبادل و جمع‌آوری اطلاعات به‌صورت محلی یا از راه دور از طریق اینترنت به‌هم متصل شده‌اند. از آنجا که این اتصالات از طریق اینترنت انجام می‌شود، در برابر تهدیدهای امنیتی در محیط IoT آسیب‌پذیرند (Das, Zeadally & He, 2008). بی‌شک، ارتباط بین موجودیت‌ها (اشیا) در متن IoT، سیستم‌ها و فرایندهای انسانی نقش فعالی دارند. اتصالات فراوان در IoT به بروز مشکلات امنیتی بسیاری منجر شده است (Sfar et al, 2018). در IoT دستگاه‌های متنوع، طیف وسیعی از داده‌ها و اطلاعات را به اینترنت متصل می‌کنند، به این دلیل طیف گسترده خطرهای امنیت اطلاعات افزایش یافته است (Hong, Park, Park, Jeon & Chang, 2018).

IoT مانند یک شمشیر دولبه عمل می‌کند که در تمامی حالات سهولت سیستم‌ها را به ارمغان نمی‌آورد، بلکه در برخی موارد مسائل امنیتی مربوط به آنها به راه‌حل‌های فوری نیاز دارند (Yang, Hao & Zhang, 2013). امنیت، برای حفاظت در دنیای فیزیکی و مجازی جزئی کلیدی محسوب می‌شود و برای بحث مشکلات موجود در امنیت و احاطه بر ویژگی‌های IoT، مزایا و محدودیت‌های آنان از طریق تجزیه‌وتحلیل ضروری است (Sha, Wei, Yang, Wang & Shi, 2018). امنیت اطلاعات مجموعه‌ای از تکنولوژی‌ها، چارچوب‌ها، سیاست‌ها و تجربه‌های مدیریتی است که بر اطلاعات اعمال می‌شود و حفظ و تأمین امنیتی اطلاعات را بر عهده دارد (Rao et al., 2018). برخی سازمان‌ها، برای برقراری امنیت، پیکربندی‌های در حال تکامل و انعطاف‌پذیر ارائه می‌دهند که این تنظیمات مبتنی بر قانون است و بر مبنای سناریوهای شبیه‌سازی‌شده برای ناسازگاری‌های امنیتی و سپس برنامه‌ریزی برای رفع آن است (Mohsin et al, 2017). پژوهشگران دانشگاهی در زمینه امنیت IoT راه‌حل‌هایی ارائه دادند که از طریق آن برای بالا بردن کیفیت امنیت IoT تلاش می‌شود (Puthal, Nepal, Ranjan & Chen, 2017).

1. Security-General-Private-Release

با توجه به سطوح تهدید، برنامه‌ریزی‌های مربوط انجام می‌شود، بدین ترتیب، ساختار و اقدامات مهم در اولویت قرار می‌گیرند، طرح مناسب برای سطح امنیت پیشنهاد می‌شود و درجه آسیب‌پذیری سیستم مشخص خواهد شد (Roy, Kim & Trivedi, 2012; Sheyner, Haines, Jha, Lippmann & Wing, 2002; Das et al, 2018). در پژوهش‌های انجام‌شده پیرامون امنیت IoT با ارائه چارچوب از عناصر ارتباطی استفاده شده و با بهره بردن از تحلیل ریسک‌های امنیتی می‌توان به کنترل پایدار برای IoT دست یافت. در این چارچوب‌ها، برای نشان دادن خطرها، از سناریوهای چندگانه بهره برده شده است و در نهایت، تشخیص سریع‌تر حملات را در پی خواهد داشت (Rathore & Park, 2018; Hossain, Islam, Ali, Kwak & Hasan, 2018; Huang, Craig, Lin & Yan; 2016; Mavropoulos, Mouratidis, Fish & Panaousis, 2019; Sun, Li, Bhuiyan, Wang & Li, 2019).



شکل ۱. انواع و انشعابات حملات عمومی با توجه به ماهیت رفتار

انواع حملات با توجه به ماهیت رفتار به دو بخش حملات فعال و غیرفعال تقسیم‌بندی می‌شوند که اجزای آن در شکل ۱ ارائه شده است (Padmavathi & Shanmugapriya, 2009; Mitrokotsa, Rieback & Tanenbaum, 2010; Douceur, 2002; Farooq, Waseem, Mazhar, Khairi & Kamal, 2015; Thakur & Chaudhary, 2013). انواع و انشعابات حملات در محاسبه احتمال رخداد حملات در سطوح کاربرد دارد. نحوه تأثیرگذاری این حملات بر سطوح در شکل ۴ مشاهده می‌شود. 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 (Yigit, Gür, Alagöz & Tellenbach, 2019). در واقع، سعی داریم حملات و تأثیر آن بر فرایندها را با تعامل بصری با تحلیل چندمعیاره بر پایه یک مدل ابتکاری مدل امنیت فرایندها به‌همراه جزئیات ارائه دهیم.

مبانی نظری پیرامون ITIL و امنیت ITIL

پروژه‌های فناوری اطلاعات شاید یکی از پروژه‌های سخت برای مدیریت باشند، زیرا با عوامل نامشهود سروکار دارند. بنابراین، بخش فناوری اطلاعات به ترکیب بهینه بسیاری از مهارت‌ها نیاز دارد که فرایندها یکی از ارکان آن هستند (Castillo, 2016). مدیریت خدمت در IT به‌وسیله ارائه‌دهنده خدمت IT از طریق اختلاط مناسب افراد، فرایندها و فناوری اطلاعات انجام می‌شود (صادقی و حسینی، ۱۳۹۲).

فرایندها به IT متکی هستند و از طریق خدمات نوآورانه IT اهمیت یافته‌اند (Beims, 2017). در نگاهی جامع‌تر در ITIL4 واژه ITIL فراتر از فرایندها معرفی شده و اصطلاح مردم و فناوری نیز به آن افزوده شده است. شیوه و تمرین در ITIL خود حاوی قابلیت‌ها، مردم، فناوری و در نهایت، فرایندهای انجام کار است (Axelos, 2019). در بررسی ساختار فرایندها باید دانست که ساختارها ارتباط میان اجزا را نشان می‌دهند، در حالی که خدمات و فرایندها به توصیف چگونگی تغییر می‌پردازند (Cannon, 2011).

در ITIL4 بر اهمیت ایجاد ارزش تأکید فروانی شده است. موارد تأکیدشده در نسخه ITIL4 ارزش، نتایج، هزینه‌ها و خطرها است (Axelos, 2019). یکی از موارد مهمی که ما را به استفاده از ITIL سوق می‌دهد، کمک به تعیین فرایندهای مهم است که از بقیه موارد از اهمیت بیشتری برخوردار است (Kumbakara, 2008). در حالی که سازمان‌ها و ارگان‌ها برای مدیریت بهتر عملکرد IT تلاش می‌کنند، ارائه چارچوب کارآمد یک راه‌حل است و مهم‌ترین چیزی که سازمان‌ها از پیاده‌سازی ITIL انتظار دارند، تراز خدمات فعلی با نیازهای احتمالی آینده است (Peak, Guynes & Kroon, 2005).

ارتا و رز[1] (۲۰۱۹) برای چگونگی دستیابی به موفقیت با مدیریت درست فرایندها با استفاده از شبیه‌سازی و مطالعه یک مورد، روش جدیدی ارائه می‌دهند. این روش، تصمیم‌گیری پیرامون فرایندها و بهبود پیوسته آنها را در پی دارد. آنها چارچوبی برای پیاده‌سازی فرایندهای ITIL با توجه به مطالعه موردی ارائه دادند و در نظر گرفتن ذی‌نفعان متناسب با اهداف را نیز توصیه می‌کنند (Orta et al, 2014). رز و همکاران رویکردی برای انتخاب فرایندهای بهینه ارائه دادند و نشان می‌دهند که چگونه این رویکرد می‌تواند به مدیران IT برای ارائه راه‌حل‌های با کیفیت کمک کند (Ruiz, Moreno, Dorronsoro & Rodriguez, 2018). استفاده از چارچوب به‌منظور بهبود عملکرد، یکی از عوامل مهم در پژوهش‌ها به شمار می‌رود. در نهایت، تقویت مسیرهای فرایندهای ITIL، تصمیم‌گیری بهینه و اثربخشی فرایندها را در پی خواهد داشت (Orta et al, 2014; Mohamed, Ribiere, O'Sullivan & Mohamed, 2008) که با ترسیم فرایندهای مربوطه می‌تواند به اتخاذ تدابیر بهتر پیرامون فرایندها کمک شایانی کند (Ahmad et al, 2013). ارائه چارچوب برای امنیت فرایندهای ITIL در محیط IoT، بهترین روش برای تأمین امنیت فرایندها است. لازم است عوامل مهم شناسایی تحلیل و ترکیب شوند. این ترکیب با ارائه مدل‌های دستی و سیستماتیک سعی در ایجاد امنیت با تخمین تأثیر حالات حدی در فعالیت‌ها به‌وسیله شبیه‌سازی با خطرهای کمتر و امکان تجربه و آزمایش یک رویداد غیرمحتمل را دارد. همچنین بهینه‌سازی تغییرات

1. Orta & ruiz

احتمالی برای مدیریت تغییر را فراهم می‌کند (آزمایش تغییر پارامتر و کالیبراسیون) و مدیران را قادر به اخذ تصمیم‌های بدون القای ریسک، هزینه و زمان را با توجه به سناریوهای موجود می‌کند.

تحلیل ارتباطات و ترکیب دو فاکتور IoT و ITIL

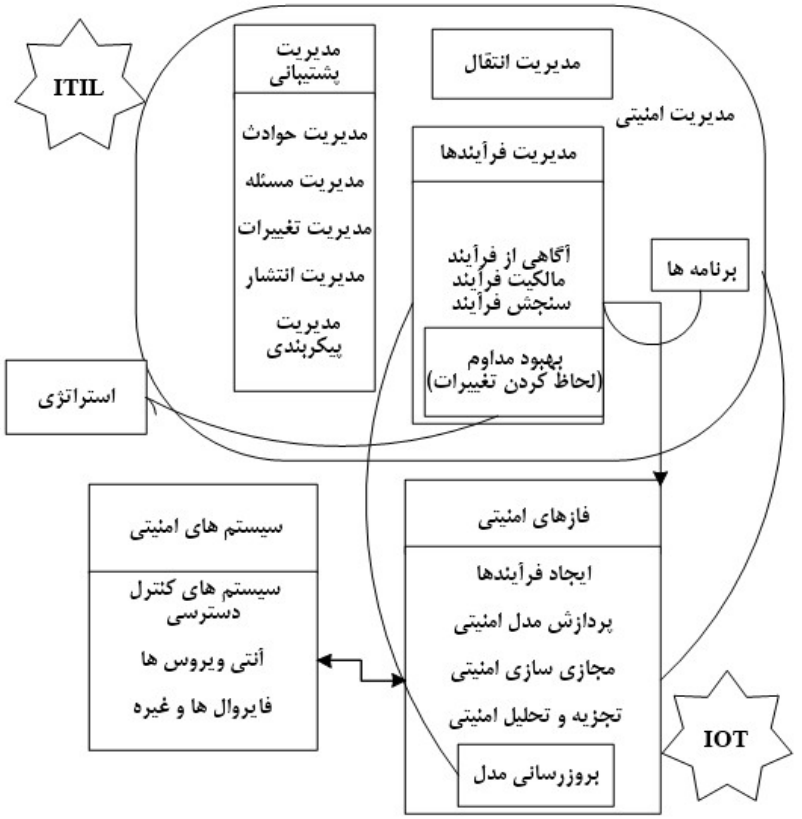
در ادامه، ارتباطات، شکل‌گیری نواحی امنیتی و چگونگی تأثیرگذاری این ارتباطات بر مطالعه موردی (تحلیل موقعیت) تحلیل می‌شود. در مجموعه یکپارچه فناوری مدیریت خدمت، به‌رغم نتایج مثبت استفاده از فناوری، اگر فناوری‌های مختلف با هم در ارتباط نباشند و نتوانند برای یکدیگر داده ارسال کنند، مدیریت عالی و مدرن به‌خوبی انجام نمی‌شود. از این رو، لازم است کلیه فناوری‌های استفاده‌شده به‌صورت یکپارچه عمل کنند (صادقی و حسینی، ۲۰۱۴). سیستم‌های تفکر تحلیلی بر اندیشیدن از خارج به داخل دلالت دارد، این در حالی است که تفکر ترکیبی بر اندیشیدن از داخل به خارج دلالت دارد و هیچ یک، ارزش دیگری را نفی نمی‌کند (رضائیان، ۱۳۹۳). ترکیب دو فاکتور IoT و ITIL تفکر داخل به خارج و تحلیل هر یک از موارد نام‌برده بر تفکر خارج به داخل اشاره دارد. شناسایی ارتباطاتی که به تشخیص ریسک‌های امنیتی منجر می‌شود، به پیش‌برد سناریوهای مختلف برای تصمیم‌گیری کمک شایانی می‌کند (Ackermann,2013).

اکثر پژوهش‌ها پیرامون امنیت IoT با تحلیل‌های کاربردی مدل‌های مختلف همراه هستند. در این پژوهش‌ها به ضعف‌ها، حملات و توصیف چگونگی دسته‌بندی‌های مختلف امنیتی پرداخته می‌شود. در برخی از این پژوهش‌ها برای تأمین و بهبود امنیت، مدل‌های شبیه‌سازی و در برخی چارچوب‌های امنیتی ارائه می‌شوند (Ge et al, 2017; Ingols et al, 2009; Saini et al, 2008; Sheyner, Haines, Jha, Lippmann & Wing, 2002). همچنین، چارچوب برای فرایندها باعث بهبود امنیت و شناسایی مسائل کلیدی داده‌ها می‌شود. از این رو، اطلاعات و فرایندها باید دسته‌بندی شوند تا استراتژی بهبود یافته و برنامه‌های مدیریتی توسعه یابند (Ge et al, 2017 Zeng, 2008; Hong et al, 2018; Robinson ,2004; Huang et al;).

چارچوب ITIL، راهنمایی مهم برای تغییرات در سازمان‌های IT است. فرایندهای ITIL شامل استراتژی، مدیریت کاتالوگ خدمت، مدیریت دانش، مدیریت حوادث و مدیریت درخواست است (Marrone, Gacenga, Cater-Steel & Kolbe, 2014; ISO/IEC) که در روابط بین ITIL و IoT مهم هستند. این تغییرات به بهبود تصمیم‌های مرتبط با فرایندها و کاهش ریسک‌ها منجر می‌شوند (Pollard & Cater-Steel, 2009).

از آنجا که ITIL، مدل مرجع مبتنی بر فرایند است، یکی از عواملی که بر موفقیت ITIL نقش زیادی دارد، مدیریت مناسب فرایندهاست. البته لازم است به موارد دیگری چون چگونگی خلق ارزش‌ها، نتایج، پیامدها و هزینه‌ها نیز توجه شود (Pollard & Cater-Steel, 2009; Haufe & Colomo-Palacios, Dzombeta, Brandis & Stantchev, 2016). طبق چارچوب امنیتی که مک‌ناتون و همکارانش برای پشتیبانی فرایندها ارائه دادند، مدیریت پشتیبانی با پنج فاکتور مدیریت حادثه، مدیریت مسئله، مدیریت تغییر، مدیریت انتشار و مدیریت پیکربندی از اجزای اصلی آن هستند. همچنین، مدیریت امنیتی و

مدیریت انتقال نیز از عوامل اصلی چارچوب ارائه‌شده است (McNaughton et al, 2010). مدیریت امنیت شامل حفاظت از منافعی است که به اطلاعات، سیستم‌ها و ارتباطات متکی است (Axelos, 2019). در مدیریت فرایند، فرایندها در اجرای موفقیت‌آمیز ITIL نقش مهمی دارند، به‌طوری که پولارد و کاتر استیل[1] (۲۰۰۹) سه عامل برای موفقیت ITIL شناسایی کردند که یکی از عوامل مهم اولویت دادن به فرایندهاست. اصول مدیریت فرایند شامل آگاهی از فرایند، مالکیت فرایند، سنجش فرایند و بهبود فرایند است (Orta & Ruiz, 2019). استراتژی خدمت راهبردی، طراحی، توسعه و پیاده‌سازی مدیریت خدمت را به‌عنوان یک منبع استراتژیک ارائه می‌دهد (Axelos, 2019; Bon, 2007). در ادامه، مدیریت برنامه مسئولیت به‌روزرسانی و حفظ تمامی پیکربندی‌های برنامه را بر عهده دارد (Castillo, 2016).



شکل ۲. تشریح روابط امنیتی IoT و ITIL (مدل دستی توضیحات ترکیبی)

1. Pollard & Cater-Steel

سیستم‌های امنیتی در IoT شامل سیستم‌ها و سرویس‌های امنیتی است. سرویس‌های امنیتی شامل سرویس‌های مشاوره، ارزیابی و عملیات سرویس هستند و سیستم‌های امنیتی شامل سیستم‌های کنترل دسترسی، آنتی ویروس‌ها و فایروال‌ها هستند (Hong et al., 2018). برای تهیه چارچوب امنیتی IoT پنج فاز پیشنهاد می‌شود که شامل پردازش داده‌ها (ایجاد فرایند)، پردازش مدل امنیتی، مجازی‌سازی امنیتی، تجزیه‌وتحلیل امنیتی و به‌روزرسانی مدل است (Ge et al, 2017).

توضیحات مندرج در امنیت دو فاکتور و تحلیل ارتباطات آنها در مدل دستی بالا مشاهده می‌شود که تعداد انشعابات ارتباطات، ورودی مدل دستی شماره ۴ است. در ادامه، استفاده از تحلیل‌های کاربردی و تحلیل مدل‌های مختلف با استفاده از مطالعه یک مورد برای شناسایی در بررسی سطوح امنیتی موارد بیان‌شده با مشخص شدن وضعیت فرایندها گراف حملات نیز تشخیص و بررسی می‌شود. استفاده از گراف حملات یکی از راه‌های مؤثر برای مسائل امنیتی IoT است (Ge et al, 2017; Ingols et al, 2009; Saini et al, 2008; Sheyner et al, 2002).

روش‌شناسی پژوهش

ساختار پایه کتابخانه در پژوهش برای ارائه مدل شبیه‌سازی از سه بخش تشکیل شده است. بخش اجرایی شبیه‌سازی شامل تجزیه‌وتحلیل دقیق و سازمان یافته عوامل مهم دخیل در امنیت دو فاکتور IoT و ITIL برای ترکیب و تحلیل دو فاکتور مطروحه، گراف حملات، تعیین نواحی و ماژول‌های امنیتی است. در این قسمت اطمینان حاصل شد که تمامی عوامل در شبیه‌سازی به درستی درگیر باشند. بخش دوم منطق مدل است که شامل معادلات، سطوح، نرخ جریان‌ها و احتمال رخداد حملات است. این قسمت با بخش اجرایی در ارتباط است. بخش سوم کتابخانه توابع است که شامل مطالعه موردی (سه دسته آزاد، دانشگاهی و سازمانی)، مدل شبیه‌سازی، آزمایش تغییر پارامتر و آزمایش کالیبراسیون است.

روند دستیابی به چارچوب پیشنهادی

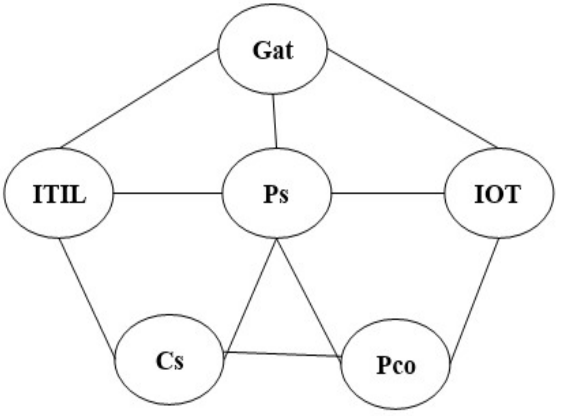
با توجه به سطوح و گراف حملات می‌توان برای سه ماژول امنیتی و ارائه چارچوب امنیتی پژوهش حاضر، چهار ناحیه امنیتی ارائه داد:

۱. حملات عمومی و تأثیر آن بر سطوح و لایه‌ها (ناحیه A)
۲. ارتباطات عمومی بین فاکتورهای بین IoT و ITIL و امنیت فرایندها (لایه B)
۳. محتوای فرایندها (ناحیه C)
۴. ماژول‌های اختصاصی و انتشار (تحت‌تأثیر مطاالعه موردی در تحلیل موقعیت) (ناحیهD)

علامت اختصاری هر یک از موارد نام‌برده در جدول ۱ ارائه شده است که در ارائه روابط، احتمالات، معادلات و مدل نهایی SGPR کاربرد دارد.

جدول ۱. معرفی عناصر استفاده‌شده و نشانه‌گذاری

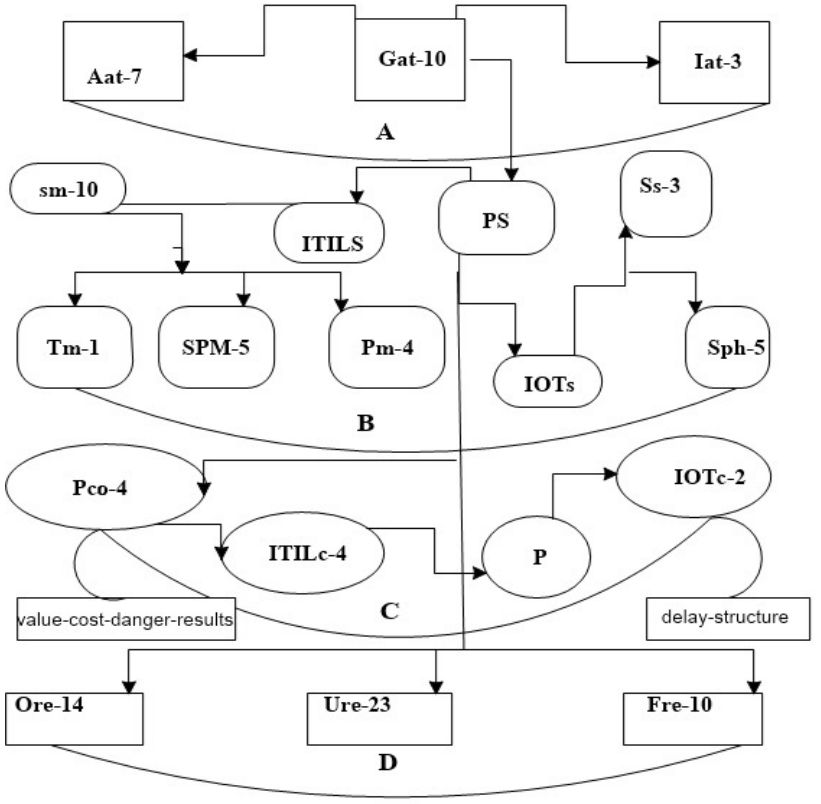
عناصر	نشانه‌گذاری	عناصر	نشانه‌گذاری	عناصر	نشانه‌گذاری
Case study	Cs	IoT Security	IoTs	Processes	P
Process content	pco	Security management	Sm	Case study attack rates	(Cs) r
Total security	Ts	Attack graph	Atg	ITIL Security	ITILs
Total research	Tre	General attacks	Gat	Process management	Pm
Research time	Ret	Active attacks	Aat	Support management	Spm
Release cost	Rec	Inactive attacks	Iat	Process security	Ps
Research	Re	Security system	Ss	Security phases	Sph
Case study time	Cst	Total processes	Tp	Organizational research	Ore
ITIL content	ITILc	Transfer management	Tm	University research	Ure
IoT content	IoTc	Free research	Fre	Each of the items used	(*) r
Attacks gragh	Atg	University research	Ure	Organizational research	Ore



شکل ۳. گراف حملات

شکل ۳ گراف حملات را نشان می‌دهد که امنیت فرایندها را تهدید می‌کند. تمام مجموعه مسیرهای حمله AP در گراف را نظر می‌گیریم. برای یک هدف مشخص از سطح $ap \in AP$ دارای یک یا چند آسیب‌پذیری است. هر فرایندی که زیرمجموعه فرایندها است. $p \in P$ بنابراین:

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



شکل ۴. مدل دستی از نحوه ارتباط موارد تأثیرگذار بر ماژول‌ها (زیربخش از گراف حملات)

شکل ۴ نحوه تأثیرگذاری حملات را با توجه به گراف حملات بر ماژول‌ها را نشان می‌دهد، اعداد کنار هر یک نمایانگر تعداد انشعابات و اعداد داخل پرانتز نشان‌دهنده تعداد انشعابات فرعی است. این انشعابات با توجه به تناسب ارتباطات و با تحلیل موقعیت تنظیم و محاسبه شده و ارائه می‌شوند. ماژول‌های امنیتی در نواحی امنیتی بالا به‌ترتیب عبارت‌اند از:

ماژول امنیتی عمومی

به‌طور اختصاصی هر یک از ماژول‌های ارائه‌شده دارای مراحل و سطوح[1] امنیتی خاصی هستند. در پویایی سیستم، وضعیت فعلی سیستم مربوط به حالت سیستم است، یعنی سطوح متغیرهای حالات سیستم هستند. با توجه به مدل دستی در شکل‌های ۲ و ۴ مسیرهای حمله به شرح ذیل است:

$p \in P$ و AP مسیرهای حمله مشخص‌شده در گراف حملات است. بنابراین:

1. Stocks

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

$IOTs = (Re) \cap (Ss, Sph) \cap (IOTsr)$

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

$ITILs = (P) \cap (Tm, Spm, Pm) \cap (ITILsr)$

$ap \in Ap, AP \in Atg, PCs \in \{Pco, (Cst, (Fre, Ure, Ore), Csc, Csr)\}$

$Cs = (Pco) \cap (Cst) \cap (Fre, Ure, Ore) \cap (Csr) \cap (Csc)$

$ap \in AP, AP \in Atg, PPco \in \{Ps, (ITILc, IoTc), Pcor\}$

$Pco = (Ps) \cap (IoTc, ITILc) \cap (Pcor)$

$ap \in AP, AP \in Atg, PPs \in \{Gat, (IOTs, ITILs), Psr\}$

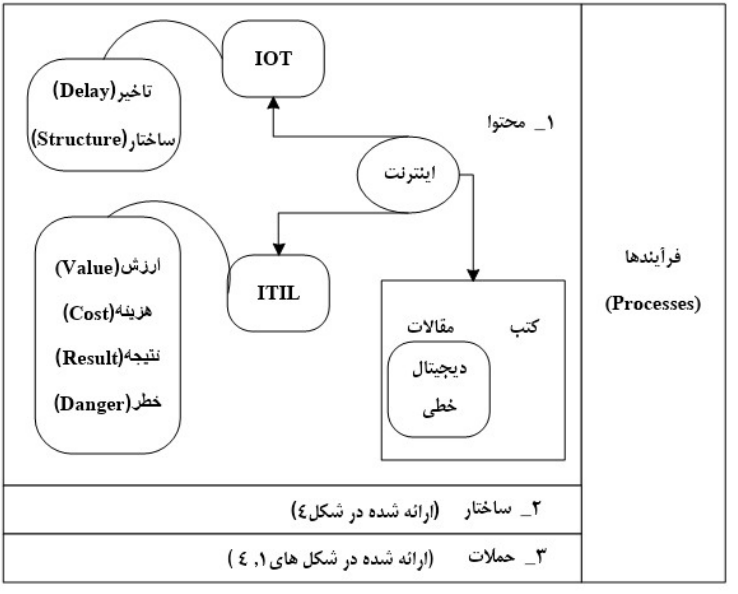
$Ps = (Gat) \cap (IoTs, ITILs) \cap (Psr)$

$ap \in AP, AP \in Atg, PGat \in \{(Aat, Iat), Gatr\}$

$Gat = (Aat, Iat) \cap (Gatr)$

$ap \in AP, AP \in Atg, PTs \in \{Cs, IOTs, ITILs, Jo, Co, Ret\}$

$Ts = (Cs) \cap (IoTs) \cap (ITILs) \cap (Jo, Co) \cap (Ret)$



شکل ۵. تشریح ماژول امنیتی عمومی فرایندها (زیر بخش گراف حملات)

در مبحث ITIL نیز همان‌طور که از نظر گذراندیم، چهار عامل ارزش، هزینه، نتایج و خطرها از عوامل مهم و تعیین‌کننده هستند. تأخیرها از خصوصیت‌های مربوط به سیستم‌های پویا هستند که هر دو جریان مواد و اطلاعات را تحت‌تأثیر قرار می‌دهند (pidd, 2016). هر یک از موارد یادشده در شکل ۵ به‌صورت عمومی در هر ماژول مطرح‌شده که از IoT و ITIL بهره می‌برد، تأثیرگذار هستند.

ماژول اختصاصی

در این پژوهش، سطوح حداکثری در هر یک از بخش‌های مطالعه موردی لحاظ شده‌اند. در حقیقت، فرض بر این است که هر یک از سطوح موجود (لااقل یک سطح) به‌نحوی ممکن است بر تأمین امنیت نهایی تأثیرگذار باشند. این سطوح در محاسبه احتمال رخداد حملات استفاده می‌شوند.

در این ماژول در تحلیل موقعیت (مطالعه موردی) در سه دسته به مطالعه و بررسی می‌پردازیم:

- دسته آزاد: شامل سیستم شخصی (امنیت وسایل، امنیت نقش‌ها و امنیت فرایندها)، انتخاب موضوع (تأیید ذی‌نفعان)، طرح پژوهش (تعریف پروژه و تأیید ذی‌نفعان)، بیان مسئله، اهداف پژوهش، اهمیت و ضرورت پژوهش و مقاله (دستاوردهای پژوهشی). تعداد این سطوحی که احتمال رخداد حملات در آنها وجود دارد، ۱۰ در نظر گرفته می‌شود.
- دسته دانشگاهی: سیستم دانشگاه (امنیت وسایل، امنیت نقش‌ها و امنیت فرایندها)، انتخاب موضوع (انتخاب دانشجو و تأیید استاد راهنما)، طرح پژوهش (تعریف پروژه، درخواست اخذ، تأیید درخواست اخذ، تأیید استاد راهنما، تأیید هیئت داوران و تأیید مشاور)، بیان مسئله، اهداف پژوهش، اهمیت و ضرورت پژوهش، تصویب پروپوزال (تأیید درخواست اخذ، تأیید شورای داوران، تأیید شورای تحصیلات تکمیلی و تأیید شورای پژوهشی)، دفاع (استادان، داوران و دانشجو) و رساله و مقاله (دستاورهای پژوهشی). تعداد سطوحی که احتمال رخداد حملات در آنها وجود دارد، ۲۳ در نظر گرفته می‌شود.
- دسته سازمانی: سیستم سازمانی (امنیت وسایل، امنیت نقش‌ها و امنیت فرایندها)، انتخاب موضوع (انتخاب سازمانی و تأیید سازمانی)، طرح پژوهش(ارائه به طرح و برنامه، طرح در کارگروه پژوهشی، اولویت طرح پژوهشی، شورای برنامه‌ریزی و توسعه و اعلام فراخوان در بازه زمانی)، بیان مسئله، اهداف پژوهش، اهمیت و ضرورت پژوهش و مقاله (دستاوردهای پژوهشی). تعداد سطوحی که احتمال رخداد حملات در آنها وجود دارد، ۱۴ سطح در نظر گرفته می‌شود.

ماژول امنیتی انتشار

انتشار دستاوردهای پژوهشی با توجه به سیاست‌های ارائه‌دهندگان در مجله، کنفرانس یا سازمان‌های اجرایی انجام می‌شود. سطوح تعدادی از ژورنال‌های مختلف و کنفرانس‌ها، ارائه شده از سوی مراجع ذیربط از تطبیق معیارهای ذی‌نفعان با ژورنال و ارسال پژوهش به مجله تا در ردیف چاپ گرفتن پژوهش (بسته به ژورنال متغیر است) برررسی شد. حداکثر سطوح برای ژورنال برابر ۲۴ سطح در نظر گرفته

می‌شود که ممکن است حملات در آن رخ دهد. بررسی سطوح حداکثری در کنفرانس در ارائه از تطبیق کنفرانس با معیارهای ذی‌نفعان تا انتشار پژوهش برابر ۸ سطح در نظر گرفته می‌شود. تأمین و تأیید موارد بیان‌شده و اهداف انتشار در سازمان، ارائه در سامانه خاص سازمان، ارگان یا نهاد است. بنابراین تأیید امنیت یادشده از طریق سازمان مربوطه انجام می‌شود و ضرورتی برای ارائه سطوح امنیتی در مرحله انتشار در این بخش نیست. در صورت تعمیم مطالعه موردی بسته به تعیین تعداد سطوح در هر یک از دسته‌ها متفاوت، تغییرپذیر، محاسبه‌شدنی و انجام‌پذیر است. در اینجا به‌کار بردن سطح خلاصه‌سازی بدین معناست که از جزئیات گمراه‌کننده دوری شده است.

ارزیابی امنیتی ماژول‌ها و یافته‌ها

معادلات

طریقه محاسبه و معادلات نرخ‌های جریان تأثیرگذار بر سطوح با توجه به شکل‌های ۴ و ۵ و موارد تأثیرگذار بر سطوح مختلف با توجه به ماژول‌های امنیتی و توضیحات مندرج در ماژول‌های اختصاصی و انتشار به‌صورت زیر محاسبه می‌شوند (نرخ جریان‌ها در مدل شبیه‌سازی کاربرد دارد):

- حملات در فاز امنیتی عمومی (ناحیه A، B و C):

$$(Gat)r = Aat * Iat$$
$$(ITILs)r = (Ms)r = Pm * Spm * Tm * P * Gatr/TP$$
$$(IoTs)r = Sph * Ss * Re * Gatr/TRE$$
$$(Ps)r = IoTs * ITILs(Sm) * Gat$$
$$(Pco)r = ITILc * IoTc * Ps$$

- حملات در فاز امنیتی اختصاصی (ناحیه D):

$$(Cs)r = Fre * Ure * Ore * Cst * Csc * Pco$$

- حملات در فاز امنیتی انتشار (ناحیه D):

$$(Ts)r = IoTs * ITILs * Jo * Co * Ret * Rec * Cs$$

تعیین احتمال رخداد حملات در هر یک از سطوح و جریان‌ها

برای تعیین احتمال رخداد حملات، احتمال وقوع رخداد حملات در هر یک از سطوح انسانی و غیرانسانی نسبت به کل احتمال وقوع حملات در تمامی سطوح سنجیده و محاسبه می‌شوند. نرخ حملات حداقلی و حداکثری در هر یک از سطوح موجود در زیربخش‌های ماژول اختصاصی با توجه به انشعابات آنها در سه دسته آزاد، دانشگاهی و سازمانی تقریباً برابر صفر است، بنابراین می‌توان از آن چشم‌پوشی کرد.

جدول ۲. پارامترها و مقادیر لحاظ‌شده در مدل SGPR

Aat=۰/۷	Cst=۲۴	ITILc=۰/۶۶	Parameters=value				
Ure=۰/۴۸۹	Jo=۰/۰۴۱	Iat=۰/۳	Ret=۶	IoTc=۰/۳۳	Spm=۰/۵	Tm=۰/۱	Ss=۰/۳۷
Ore=۰/۲۱	Csc=۱۵۰۰	Co=۰/۱۲۵	Tp=۲۰۰۰۰	TRE=۱۰۰۰۰	Fre=۰/۲۹۷	Sph=۰/۶۲۵	Pm=۰/۴

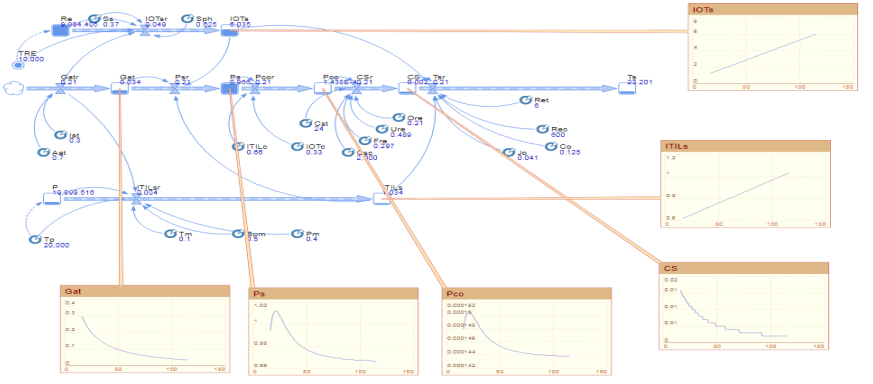
احتمال وقوع حملات در سطوح مختلف در جدول ۲ با توجه به انشعابات موجود در شکل‌های ۲، ۴ و ۵ مشاهده می‌شود. این مقادیر در مدل شبیه‌سازی SGPR لحاظ می‌شوند.

مشخص کردن سطوح و جریان‌ها

مقادیر تأثیرگذار، عناوینی هستند که با کلمه نرخ مشخص می‌شوند و به‌عنوان جریان‌های تأثیرگذار در مدل به‌کار می‌روند. سطوح، مواردی هستند که از جریان‌ها تأثیر می‌پذیرند، هرچند در مواردی ممکن است جریان‌ها از سطوح تأثیرگذار باشند. در شکل‌های ۶ و ۷ به‌وضوح سطوح، جریان‌ها، پارامترهای تأثیرگذار و نرخ جریان‌ها مشخص است.

مدل‌سازی سیستم‌های پویا

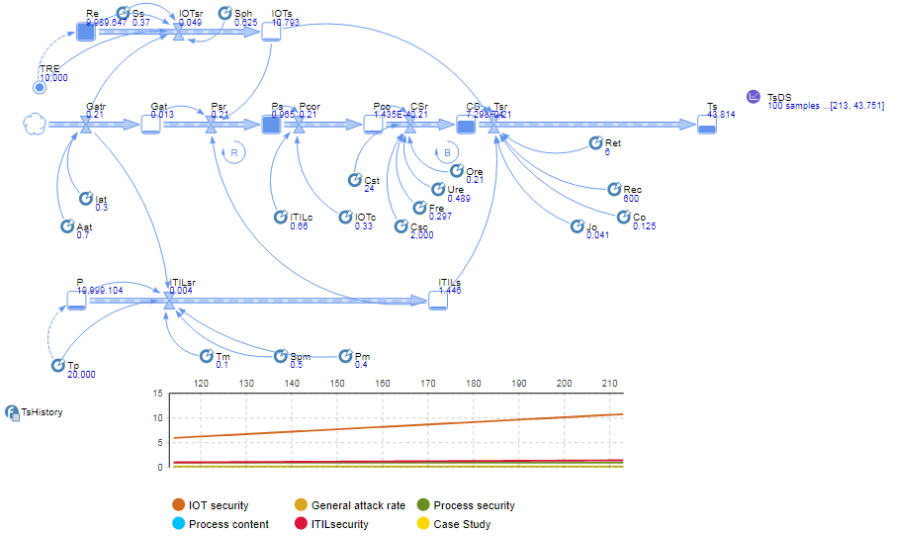
با مشخص شدن سطوح و جریان‌ها و با علم به این موضوع که هر دو می‌توانند بر یکدیگر تأثیرگذار باشند، به مدل شبیه‌سازی SGPR (مدل امنیتی با سه ماژول عمومی، اختصاصی و انتشار) اقدام می‌کنیم. با توجه به معادلات رخداد حملات محاسبه نرخ جریان‌ها در فازهای مختلف از آن طریق محاسبه می‌شود که در شکل‌های ۶ و ۷ لحاظ می‌شوند. واحد زمانی در مدل‌ها ماه و واحد هزینه دلار است.



شکل ۶. اجرای مدل SGPR در مرحله اول

در شکل ۶ با افزایش امنیت فرایندها، امنیت در آنها کاهش می‌یابد، به همین دلیل از حلقه‌های بازخوردی متعادل‌کننده استفاده می‌کنیم. تعداد پیوندهای منفی ناموزون در Cs با کاهش Gat امنیت

فرایندها افزایش می‌یابد، بنابراین به حلقه تقویت‌کننده نیاز داریم. حلقه تقویت‌کننده را در Psr قرار می‌دهیم، سپس مدل را اجرا می‌کنیم. این حلقه‌ها را تعادل یا تقویت می‌کنیم. این حلقه‌ها بهترین ابزار برای ترسیم روند پویایی سیستم بین متغیرهای مهم هستند. شکل ۷ مدل را با اضافه کردن حلقه‌ها و پالت زمانی نشان می‌دهد که 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.



شکل ۷. اجرای مدل شبیه سازی SGPR بعد از اضافه کردن حلقه‌ها و پالت زمانی

آزمایش تغییر پارامتر

متغیر کردن پارامترها را در سه فاز عمومی، اختصاصی و انتشار انجام می‌دهیم. به‌دلیل پرداختن به بررسی وضعیت پارامترها، به متغیر کردن پارامترهایی اقدام می‌کنیم که بر سطوح فرایندها تأثیرگذار هستند.

- متغیر کردن پارمترهای فاز امینتی عمومی: متغیر کردن پارامترها در این فاز در سه مرحله انجام می‌شوند:

۱. مرحله نخست فاز عمومی: دو پارامتر تأثیرگذار بر سطح Gat متغیر شده است. تغییر محدوده این دو پارامتر بر تمامی سطوح تأثیرگذار است.

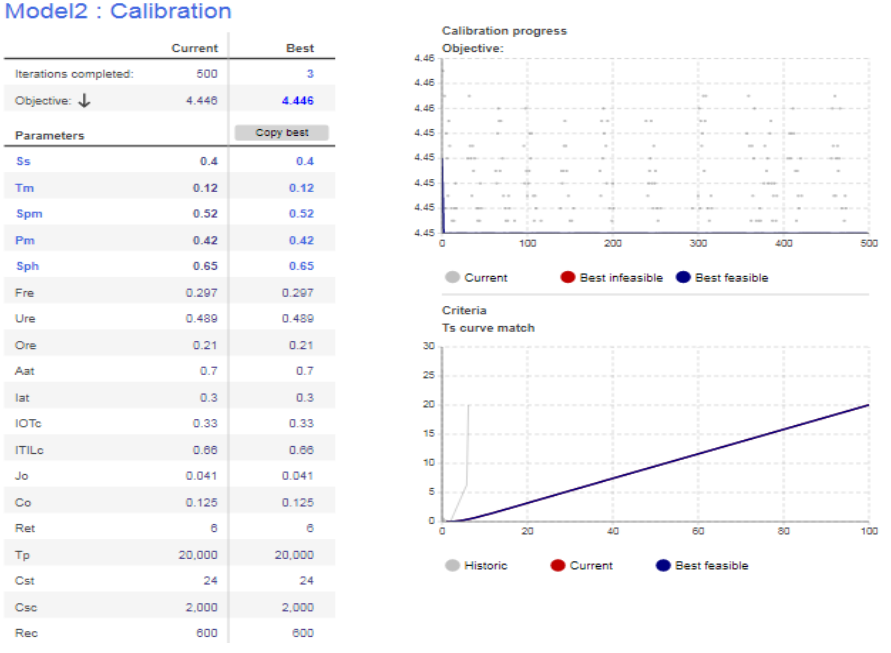
۲. مرحله دوم فاز عمومی: در این مرحله پارامترهای تأثیرگذار بر سطوح ITIL و IoT متغیر شده است. این تغییر پارامترها بر IoTs، ITILs و Cs تأثیر دارد و تغییراتی را در نمودار آنها به‌وجود می‌آورند. سایر سطوح تقریباً بدون تغییر باقی می‌مانند.

۳. مرحله سوم فاز عمومی: در این مرحله پارامترهای تأثیرگذار بر Gat و Pco متغیر شده است. تغییرات بر تمامی سطوح تأثیر دارند.

- متغیر کردن پارامترها فاز امنیتی اختصاصی: تغییر محدوده در پارامترهای تأثیرگذار بر Cs انجام شده است. تأثیر تغییرات در Pco مشاهده می‌شود و بقیه نمودارهای تغییرات در سطوح تقریباً بدون تغییر باقی می‌مانند.
- متغیر کردن محدوده پارامترهای فاز امنیتی انتشار: پارامترها تأثیرگذار بر Ts متغیر شده است. تأثیر این تغییرات در Cs مشاهده می‌شود و بقیه سطوح تقریباً بدون تغییر باقی می‌مانند.
- متغیر کردن محدوده پارامترهای زمان و هزینه: پارامترهای تأثیر زمان و هزینه متغیر شده است. این تأثیر تغییرات در Pco مشاهده می‌شود و تقریباً بقیه سطوح بدون تغییر باقی می‌مانند.

آزمایش کالیبراسیون

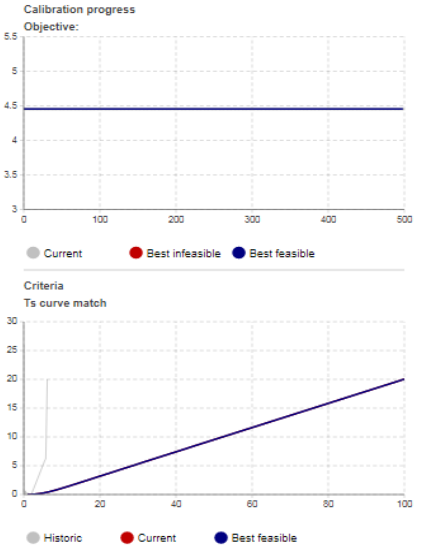
آزمایش کالیبراسیون به‌صورت تکراری مدل را اجرا می‌کند، خروجی مدل را با داده‌های تاریخی موجود در پایگاه داده TSDS در مدل مقایسه می‌کند و سپس مقادیر پارامتر را تغییر می‌دهد. بعد از انجام یک سری آزمایش مشخص می‌شود که مقادیر کدام پارامترها با نتایج مطابقت بیشتری دارد. آزمایش کالیبراسیون را برای سه فاز عمومی، اختصاصی و انتشار و همچنین هزینه و زمان به‌طور جداگانه انجام می‌دهیم. شکل‌های ۸، ۹، ۱۰ و ۱۱ آزمایش کالیبراسیون را در چهار مرحله و سه فاز امنیتی نشان می‌دهند.



شکل ۸. آزمایش کالیبراسیون در فاز امنیتی عمومی بعد از جایگزین کردن بهترین گزینه‌ها

Model2 : Calibration1

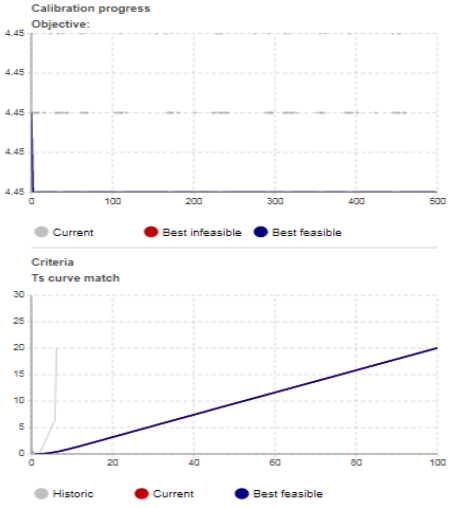
	Current	Best
Iterations completed:	500	3
Objective: ↓	4.453	4.453
Parameters		Copy best
Ss	0.37	0.37
Tm	0.1	0.1
Spm	0.5	0.5
Pm	0.4	0.4
Sph	0.625	0.625
Fre	0.35	0.35
Ure	0.51	0.51
Ore	0.23	0.23
Aat	0.7	0.7
Iat	0.3	0.3
IOTc	0.33	0.33
ITILc	0.66	0.66
Jo	0.041	0.041
Co	0.125	0.125
Ret	6	6
Tp	20,000	20,000
Cst	24	24
Csc	2,000	2,000
Rec	600	600



شکل ۹. آزمایش کالیبراسیون فاز امنیتی اختصاصی بعد از جایگزین کردن بهترین گزینه‌ها

Model2 : Calibration2

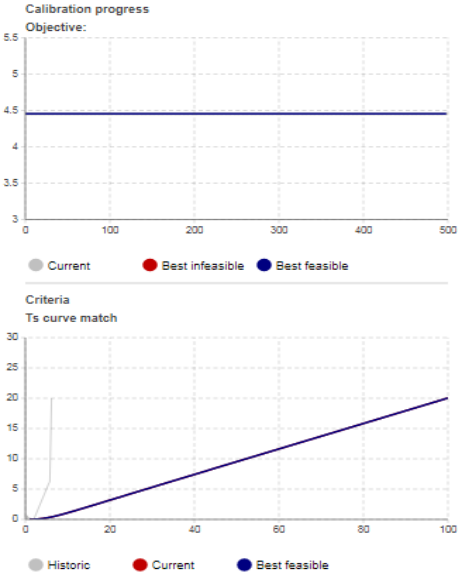
	Current	Best
Iterations completed:	500	3
Objective: ↓	4.452	4.452
Parameters		Copy best
Ss	0.37	0.37
Tm	0.1	0.1
Spm	0.5	0.5
Pm	0.4	0.4
Sph	0.625	0.625
Fre	0.297	0.297
Ure	0.489	0.489
Ore	0.21	0.21
Aat	0.7	0.7
Iat	0.3	0.3
IOTc	0.33	0.33
ITILc	0.66	0.66
Jo	0.043	0.043
Co	0.15	0.15
Ret	6.2	6.2
Tp	20,000	20,000
Cst	26	26
Csc	2,000	2,000
Rec	600	600



شکل ۱۰. آزمایش کالیبراسیون فاز امنیتی انتشار بعد از جایگزین کردن بهترین گزینه‌ها

Model2 : Calibration3

	Current	Best
Iterations completed:	500	3
Objective: ↓	4.453	4.453
Parameters		Copy best
Ss	0.37	0.37
Tm	0.1	0.1
Spm	0.5	0.5
Pm	0.4	0.4
Sph	0.625	0.625
Fre	0.297	0.297
Ure	0.489	0.489
Ore	0.21	0.21
Aat	0.7	0.7
Iat	0.3	0.3
IOTc	0.33	0.33
ITILc	0.66	0.66
Jo	0.041	0.041
Co	0.125	0.125
Ret	6.2	6.2
Tp	20,000	20,000
Cst	29.948	30
Csc	2,001.941	2,002
Rec	602	602



شکل ۱۱. آزمایش کالیبراسیون زمان و هزینه بعد از جایگزین کردن بهترین گزینه‌ها

پنج پارامتر از فاز عمومی Ss، Sph، Tm، Pm و Spm، سه پارامتر از فاز اختصاصی Fre، Ure و Ore و دو پارامتر از فاز انتشار Jo و CO و Ret، Rec، Cst و Csc در بخش زمان و هزینه در چهار مرحله کالیبره شدند. بعد از انجام آزمایش کالیبراسیون، بهترین گزینه‌های موجود در آزمایش نمایش داده می‌شود که می‌توانیم آنها را جایگزین کنیم. بعد از انجام آزمایش در مرحله انتشار دو پارامتر زمانی به‌همراه دو پارامتر موجود در این فاز نیز کالیبره شدند که به‌همراه سایر گزینه‌های بهینه‌شده نتایج به رنگ آبی و پررنگ دیده می‌شوند.

در مدل شبیه‌سازی SGPR از اعداد مندرج در جدول ۲ استفاده شده است. نتایج به‌دست‌آمده در آزمایش کالیبراسیون بهترین گزینه‌ها را برای شبیه‌سازی سیستم‌های پویا ارائه می‌دهند که می‌توانند در مدل جایگزین شوند. می‌توان گفت احتمالاً عوامل مؤثر دیگری وجود دارند که می‌توان با بررسی‌های بیشتر به اعداد مندرج دست یافت. هرچند اعداد استفاده‌شده در مدل به گزینه‌های بهینه در آزمایش کالیبراسیون بسیار نزدیک هستند. این آزمایش نشان می‌دهد که اعداد استفاده‌شده مقادیر قابل قبولی هستند.

نتیجه‌گیری

در این پژوهش، چارچوب امنیتی فرایندهای ITIL در محیط IoT بر پایه مدل شبیه‌سازی ارائه شد. پژوهش حاضر در سه مرحله تکامل یافت. مرحلهٔ نخست، مطالعه، بررسی و تجزیه‌وتحلیل دقیق دو فاکتور IoT و ITIL. مرحلهٔ دوم، تجزیه‌وتحلیل روابط بین IoT و ITIL، ارائه مدل‌های دستی و گراف حملات و مرحلهٔ سوم، ارائه مدل شبیه‌سازی و چارچوب امنیتی. در حقیقت داده‌های خام برای رسیدن به نتایج روند به‌دست‌آوردن تعداد انشعابات حمله، محاسبهٔ احتمال رخداد حمله، حذف مقادیر نزدیک به صفر، لحاظ کردن احتمالات و سطوح در مدل شبیه‌سازی، درج مقادیر در پایگاه داده TSDS در مدل SGPR، آزمایش تغییر پارامتر و آزمایش کالیبراسیون برای ارائه مقادیر بهینه و جای‌گذاری در مدل SGPR را طی کرده است. با وجود انعطاف‌پذیری‌های مدل ارائه‌شده، مطالعه موردی و گام‌های مدل شبیه‌سازی (مشخص کردن نواحی امنیتی، معادلات، سطوح، پارامترها، نرخ جریان‌ها) در صورت ضرورت می‌توان چارچوب‌های انحصاری با تغییر در این گام‌ها را با جزئیات بیشتر ارائه کرد. در نهایت، می‌توان گفت با توجه به دلیل گستردگی و دقت در ارائه موارد یادشده برای مدل شبیه‌سازی اعداد احتمال رخداد حملات به گزینه‌های بهینه در آزمایش کالیبراسیون نزدیک است و روند انجام شبیه‌سازی را تأیید می‌کنند.

پیشنهادهای پژوهشگر

پیشنهادهای حاصل از پژوهش حاضر برای تأمین امنیت

۱. در صورت ترکیب فاکتورهای IoT و ITIL به اشتراک‌ها و نحوه تأثیر هر یک از عوامل بر یکدیگر توجه شود. پژوهش‌های گسترده و نظام‌مند به ارائه ارتباطات بهینه، ترکیب فاکتورها، ارائه انشعابات و مدل شبیه‌سازی کمک شایانی می‌کند. توجه شود که آزمایش تغییر پارامتر برای مدیریت تغییر در امنیت فرایندها می‌تواند به‌طور گسترده استفاده شود.

۲. سرمایه‌گذاری نکردن برای ایجاد سطوح غیرضروری به‌دلیل کوچک بودن احتمال رخداد حمله در سطوح یادشده (تقریباً برابر صفر). بالا بردن سطوح در جزئیات و زیربخش‌ها کمکی به ایجاد امنیت نمی‌کند.

پیشنهادها برای پژوهشگران آینده

۱. بررسی کیفی و کمی آسیب‌ها و تهدیدهای امنیتی در مدل‌های مختلف ارائه‌شده مدیریت امنیتی برای فرایندها و نزدیک شدن به گزینه‌های بهینه ارائه‌شده در آزمایش کالیبراسیون.

۲. بررسی دقیق‌تر و عمیق‌تر مسائل اقتصادی و زمانی در تأمین امنیت و ارائه دستاوردهای پژوهشی. این بررسی بر تکمیل و محاسبه احتمال رخداد حملات و ارائه مدل شبیه‌سازی نتایج شایان توجهی به‌دنبال خواهد داشت.

فهرست منابع

رضائیان، علی (۱۳۹۳). *مبانی سازمان و مدیریت*. تهران: نشر سمت.

صادقی، محمد؛ حسینی، علی (۱۳۹۲). *مدیریت فناوری اطلاعات (جلد اول)*. اصفهان: نشر مانی.

Ackermann, T., *IT Security Risk Management: Perceived IT Security Risks in the Context of Cloud Computing*2013: Springer Gabler.

Ahmad, N., Amer, N. T., Qutaifan, F., & Alhilali, A. (2013). Technology adoption model and a road map to successful implementation of ITIL. *Journal of Enterprise Information Management*, 26(5).

Axelos. (2019). *ITIL4 foundation*. TSO publishers.

Beims, M. (2017). ITIL: Wundermittel für IT-Services? *Wirtschaftsinformatik & Management*, *9*(1), 70-79.

Bon, J.V. (2007). *ITIL V3 - A Pocket Guide (Best Practice) Kindle Edition*. Van Haren Publishing.

Cannon, D. (2011). *Itil service strategy*. TSO, The Stationery Office; Second edition.

Castillo, F. (2016). IT Portfolio Management. In *Managing Information Technology* (pp. 211-227). Springer, Cham.

Das, A. K., Zeadally, S., & He, D. (2018). Taxonomy and analysis of security protocols for Internet of Things. *Future Generation Computer Systems*, *89*, 110-125.

Douceur, J. R. (2002, March). The sybil attack. In *International workshop on peer-to-peer systems* (pp. 251-260). Springer, Berlin, Heidelberg.

Farooq, M. U., Waseem, M., Mazhar, S., Khairi, A., & Kamal, T. (2015). A review on internet of things (IoT). *International journal of computer applications*, *113*(1), 1-7.

French, W. L., & Bell, C. (1995). *Organization development: Behavioral science interventions for organization improvement*. Pearson Educación.

Ge, M., Hong, J. B., Guttmann, W., & Kim, D. S. (2017). A framework for automating security analysis of the internet of things. *Journal of Network and Computer Applications*, *83*, 12-27.

Han, K. H., Kang, J. G., & Song, M. (2009). Two-stage process analysis using the process-based performance measurement framework and business process simulation. *Expert systems with applications*, *36*(3), 7080-7086.

Haufe, K., Colomo-Palacios, R., Dzombeta, S., Brandis, K., & Stantchev, V. (2016). A process framework for information security management.

Hong, S., Park, S., Park, L. W., Jeon, M., & Chang, H. (2018). 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*, *82*, 769-782.

Hossain, M., Islam, S. R., Ali, F., Kwak, K. S., & Hasan, R. (2018). An Internet of Things-based health prescription assistant and its security system design. *Future generation computer systems*, *82*, 422-439.

Huang, X., Craig, P., Lin, H., & Yan, Z. (2016). SecIoT: a security framework for the Internet of Things. *Security and communication networks*, *9*(16), 3083-3094.

Ingols, K., Chu, M., Lippmann, R., Webster, S., & Boyer, S. (2009, December). Modeling modern network attacks and countermeasures using attack graphs. In *2009 Annual Computer Security Applications Conference* (pp. 117-126). IEEE.

ISO/IEC, Corporate governance of information technology in 385002008.

Jang, J., Jung, I. Y., & Park, J. H. (2018). An effective handling of secure data stream in IoT. *Applied Soft Computing*, *68*, 811-820.

Kumbakara, N. (2008). Managed IT services: the role of IT standards. *Information Management & Computer Security*.

Law, A. M., Kelton, W. D., & Kelton, W. D. (2000). *Simulation modeling and analysis* (Vol. 3). New York: McGraw-Hill.

Marrone, M., Gacenga, F., Cater-Steel, A., & Kolbe, L. (2014). IT service management: A cross-national study of ITIL adoption. *Communications of the association for information systems*, *34*(1), 49.

Mavropoulos, O., Mouratidis, H., Fish, A., & Panaousis, E. (2019). Apparatus: A framework for security analysis in internet of things systems. *Ad Hoc Networks*, *92*, 101743.

McNaughton, B., Ray, P., & Lewis, L. (2010). Designing an evaluation framework for IT service management. *Information & management*, *47*(4), 219-225.

Mitrokotsa, A., Rieback, M. R., & Tanenbaum, A. S. (2010). Classification of RFID attacks. *Gen*, *15693*(14443), 14.

Mohamed, M. S., Ribiere, V. M., O'Sullivan, K. J., & Mohamed, M. A. (2008). The restructuring of the information technology infrastructure library (ITIL) implementation using knowledge management framework. *Vine*.

Mohsin, M., Anwar, Z., Zaman, F., & Al-Shaer, E. (2017). IoTChecker: A data-driven framework for security analytics of Internet of Things configurations. *Computers & Security*, *70*, 199-223.

Orta, E., & Ruiz, M. (2019). Met4ITIL: A process management and simulation-based method for implementing ITIL. *Computer Standards & Interfaces*, *61*, 1-19.

Orta, E., Ruiz, M., Hurtado, N., & Gawn, D. (2014). Decision-making in IT service management: a simulation-based approach. *Decision Support Systems*, *66*, 36-51.

Padmavathi, D. G., & Shanmugapriya, M. (2009). A survey of attacks, security mechanisms and challenges in wireless sensor networks. *arXiv preprint arXiv:0909.0576*.

Peak, D., Guynes, C. S., & Kroon, V. (2005). Information technology alignment planning—a case study. *Information & management*, *42*(5), 635-649.

Pidd, M. (2004). *Computer simulation in management science* (No. 5th). John Wiley and Sons Ltd.

Pollard, C., & Cater-Steel, A. (2009). Justifications, strategies, and critical success factors in successful ITIL implementations in US and Australian companies: an exploratory study. *Information systems management*, *26*(2), 164-175.

Puthal, D., Nepal, S., Ranjan, R., & Chen, J. (2017). A dynamic prime number based efficient security mechanism for big sensing data streams. *Journal of Computer and System Sciences*, *83*(1), 22-42.

Rao, M., Newe, T., Omerdic, E., Kaknjo, A., Elgenaidi, W., Mathur, A., ... & Toal, D. (2018). Bump in the wire (BITW) security solution for a marine ROV remote control application. *Journal of information security and applications*, *38*, 111-121.

Rathore, S., & Park, J. H. (2018). Semi-supervised learning based distributed attack detection framework for IoT. *Applied Soft Computing*, *72*, 79-89.

Robinson, S., *Towards a model of franchises for community telecentres in Latin America.* M. Bonilla y G. Cliché, G.(Eds.), Internet and Society in Latin America and the Caribbean, 2004: p. 337,361.

Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of security and privacy in distributed internet of things. *Computer Networks*, *57*(10), 2266-2279.

Roy, A., Kim, D. S., & Trivedi, K. S. (2012). Attack countermeasure trees (ACT): towards unifying the constructs of attack and defense trees. *Security and Communication Networks*, *5*(8), 929-943.

Ruiz, M., Moreno, J., Dorronsoro, B., & Rodriguez, D. (2018). Using simulation-based optimization in the context of IT service management change process. *Decision Support Systems*, *112*, 35-47.

Saini, V., Duan, Q., & Paruchuri, V. (2008). Threat modeling using attack trees. *Journal of Computing Sciences in Colleges*, *23*(4), 124-131.

Sfar, A. R., Natalizio, E., Challal, Y., & Chtourou, Z. (2018). A roadmap for security challenges in the Internet of Things. *Digital Communications and Networks*, *4*(2), 118-137.

Sha, K., Wei, W., Yang, T. A., Wang, Z., & Shi, W. (2018). On security challenges and open issues in Internet of Things. *Future Generation Computer Systems*, *83*, 326-337.

Sharp, A., & McDermott, P. (2009). *Workflow modeling: tools for process improvement and applications development*. Artech House.

Sheyner, O., Haines, J., Jha, S., Lippmann, R. & Wing, J.M. (2002). *Automated generation and analysis of attack graphs.* Paper presented at the Proceedings 2002 IEEE Symposium on Security and Privacy.

Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. *Computer networks*, *76*, 146-164.

Stergiou, C., Psannis, K. E., Kim, B. G., & Gupta, B. (2018). Secure integration of IoT and cloud computing. *Future Generation Computer Systems*, *78*, 964-975.

Sun, P., Li, J., Bhuiyan, M. Z. A., Wang, L., & Li, B. (2019). Modeling and clustering attacker activities in IoT through machine learning techniques. *Information Sciences*, *479*, 456-471.

Thakur, B. S., & Chaudhary, S. (2013). Content sniffing attack detection in client and server side: A survey. *International Journal of Advanced Computer Research*, *3*(2), 7.

White, G., Nallur, V., & Clarke, S. (2017). Quality of service approaches in IoT: A systematic mapping. *Journal of Systems and Software*, *132*, 186-203.

Yang, J.-C., Hao P., & Zhang, X. (2013). Enhanced Mutual Authentication Model Of Iot. *The Journal of China Universities of Posts And Telecommunications*, 20, 69-74.

Yiğit, B., Gür, G., Alagöz, F., & Tellenbach, B. (2019). Cost-aware securing of IoT systems using attack graphs. *Ad Hoc Networks*, *86*, 23-35.

Zeng, J. (2008). A case study on applying ITIL availability management best practice. *Contemporary Management Research*, 4(4).

A Framework for Securing Information Technology Infrastructure Library Processes in the Internet of Thing Environment

Akram Ghanaee
Ph. D Candidate, Department of Information Technology Management, Qazvin Branch, Islamic Azad University, Qazvin, Iran

Mohamadreza Sanaei[*1]
Assistant Prof., Department of Information Technology Management, Qazvin Branch, Islamic Azad University, Qazvin, Iran

Javad Mehrabi
Assistant Prof., Department of Public Administration, Qazvin Branch, Islamic Azad University, Qazvin, Iran

Abstract
Security of information technology infrastructure library processes needs to provide intelligent solutions to advance goals and prevent vulnerabilities, given the stimuli in the IoT environment. To ensure security, proper management is needed to maximize security levels so that complex paths can be eliminated, performance improved, the information technology infrastructure library process structure optimized, and ultimately the goals achieved. The present study is based on a detailed analysis of relationships, manual and systematic models by studying the security of research achievements in three categories: free, academic and organizational. We consider the probability of attacks in processes in four areas and three general modules, specific, propagation by analyzing security scenarios and with maximum levels in the simulation model. Also, the maximum levels in the case study are dedicated security module in free category 10, academic category 23, organizational category 14 and in publication security module, 24 levels for journal and 8 levels for conference. In determining the probability of an attack occurring, probabilities that are negligible and close to zero are eliminated. Then, based on the available information, a simulation model is presented, parameter change testing and calibration are performed, and the best possible values are determined in accordance with the data. This research tries to create security by estimating the effect of limit states in processes by simulation by providing manual and systematic models. It also provides optimization of possible changes for change management (parameter change testing and calibration) and enables managers to make decisions without inducing risk, cost and time according to existing scenarios.

Keywords: IoT, ITIL, Process Security, Framework, Simulation.

1. Corresponding Author: mohamadrezasanaei@gmail.com