Journal of Electronical & Cyber Defence
Vol. 9, No. 4, 2022, Serial No. 36

The Automated Security Evaluation of Threat Paths Based on Petri Nets

M. A. Ramazanzadeh[1], B. Barzegar[2*], H. Motameni[3]

*Department of Computer Engineering, Babol Branch, Islamic Azad University, Babol, Iran

(Received: 10/08/2021, Accepted: 16/11/2021)

ABSTRACT

The key challenge to be well addressed in case of emerging technologies such as the Internet of Things, Internet of Transportation, e-Health, etc. is the security. Ignoring this challenge can sometimes cause irreparable personal and financial damage to human beings in everyday life. On the other hand, to identify and extract security requirements and potential threats in the design phase of large-scale and interactive systems, there is a need to model the threats. The problem is that the existing modelling methods are mostly manual, which are inherently associated with errors, cost, time consumption, and failure to evaluate all conceivable possibilities. The present paper proposes a new method, called "Automated Security Evaluation of Threat Paths", as an automated solution to the problem of identifying and extracting potential threats. In the proposed method, by adding new capabilities such as conditional probability and security to Petri Nets, it is possible not only to automatically generate the threat paths, but also to automatically evaluate the security of threat models in both quantitative and qualitative ways. In this paper, the performance of the proposed method was evaluated under different security scenarios, and the results showed that, compared to other existing methods, the proposed method offers a higher level of security assurance and also, it is fully automated, unlike the existing methods .

Keywords: Security requirements; Threat modelling; Automated evaluation; Threat path; Reachability graph; Petri Nets

* Corresponding Author Email: barzegar@iauns.ac.ir

نشریه علمی "پدافند الکترونیکی و سایبری"
سال نهم، شماره ۴، زمستان ۱۴۰۰، ص ۹۸- ۸۷

علمی- پژوهشی

ارزیابی امنیتی خودکار مسیرهای تهدید مبتنی بر شبکه‌های پتری

محمدعلی رمضان‌زاده[۱]، بهنام برزگر[۲*]، همایون موتمنی[۳]

۱- دانشجوی دکتری، گروه کامپیوتر، دانشکده فنی مهندسی، دانشگاه آزاد اسلامی واحد ساری، ساری،

۲- استادیار، گروه کامپیوتر، دانشکده فنی مهندسی، دانشگاه آزاد اسلامی واحد بابل، بابل،

۳- دانشیار، گروه کامپیوتر، دانشکده فنی مهندسی، دانشگاه آزاد اسلامی واحد ساری، ساری، ایران

(دریافت: ۱۴۰۰/۰۵/۱۹، پذیرش: ۱۴۰۰/۰۸/۲۵)

چکیده

چالش امنیت کلید واژه مشترک و بسیار مهم در میان فناوری‌های نوظهور مانند اینترنت اشیا، اینترنت وسایل حمل و نقل، سلامت الکترونیکی و غیره می‌باشد و عدم توجه به این چالش، گاهی صدمات جانی و مالی جبران ناپذیری برای انسان‌ها در زندگی روزمره ایجاد خواهد کرد. از سویی دیگر، شناسایی و استخراج نیازمندی‌های امنیتی و تهدیدهای احتمالی در سیستم‌های مقیاس بزرگ و تعاملی در فاز طراحی نیازمند مدل‌سازی تهدیدها می‌باشد که روش‌های موجود بیشتر به‌صورت دستی همراه با خطا، صرف هزینه، زمان و عدم ارزیابی تمام احتمال‌های ممکن می‌باشد. روش پیشنهادی با نام ارزیابی امنیتی خودکار مسیرهای تهدید به‌عنوان راه‌حلی خودکار برای شناسایی و استخراج تهدیدهای احتمالی ارائه‌شده است. در روش پیشنهادی با افزودن قابلیت‌های جدید مانند، احتمال شرطی و امنیت به شبکه‌های پتری امکان تولید خودکار مسیرهای تهدید و ارزیابی امنیتی خودکار به‌صورت کمی وکیفی از مدل‌های تهدید ایجاد شده است. روش ارائه‌شده با سناریوهای مختلف امنیتی سنجش و ارزیابی شده و نتایج به‌دست آمده نشان می‌دهد که روش پیشنهادی در مقایسه با سایر روش‌های موجود تمام خودکار و دارای تضمین امنیتی سطح بالا می‌باشد.

واژه‌های کلیدی: نیازمندی‌های امنیتی، مدل‌سازی تهدید، ارزیابی خودکار، مسیر تهدید، گراف دسترسی، شبکه‌های پتری

۱- مقدمه

توسعه سریع سیستم‌های مبتنی بر اینترنت اشیا (IoT) راه را برای زندگی آسان هموار کرده است [۱]. هدف اینترنت اشیا همکاری و تعامل سیستم‌های سخت‌افزاری و نرم‌افزاری مختلف با یکدیگر می‌باشد [۳-۲] که در این میان، اینترنت وسایل حمل و نقل (IoV) به‌عنوان یکی از موضوع‌های مهم در اینترنت اشیا شناخته می‌شود. هدف IoV اطمینان از حمل و نقل روان، ایمنی و کاهش تصادف‌های جاده‌ای می‌باشد. اما امنیت چالش بسیار مهم در آن می‌باشد که انواع مختلف حمله‌ها به‌این فناوری، موقعیت‌های خطرناکی را برای زندگی انسان‌ها ایجاد می‌کند [۶- ۴]. یکی دیگر از موضوع‌های مهم در اینترنت اشیا، مراقبت‌های سلامت می‌باشد این سیستم‌ها، نظارت و کنترل شاخص‌های سلامت انسان را به‌تیم پزشکی گزارش می‌دهند. کاربرد این فناوری جان بسیاری از انسان‌ها را نجات می‌دهد با این حال، به‌دلیل محدودیت‌های دستگاه‌های اینترنت اشیا، بسیاری از آنها دارای آسیب‌پذیری‌های فراوان می‌باشند که این آسیب‌پذیری‌ها آنها را مستعد حمله‌های مختلف می‌کند [۸- ۷]. از سویی دیگر، سیستم‌های مراقبت سلامت به‌عنوان سیستم‌های پرهزینه و پیچیده شناخته می‌شوند که داده‌های آن به سطح بالایی از تضمین امنیت و حفظ حریم خصوصی نیاز دارند [۹].

مسئله امنیت یک چالش اساسی در سیستم‌های مبتنی بر اینترنت اشیا می‌باشند که باید حل شود. اکثر مدل‌های پیشنهادی موجود در اینترنت اشیا به ندرت ریسک‌های امنیتی و تهدیدهای احتمالی را در نظر می‌گیرند [۱۰].

به‌منظور کاهش یا پیشگیری از صدمه‌های جانی، مالی و حفظ ایمنی انسان‌ها در بکارگیری فناوری‌های جدید مانند: IoT ، IoV، سلامت الکترونیکی، لازم است تا برخلاف روش‌های موجود، از روش‌های خودکار با تضمین امنیتی سطح بالا به‌منظور استخراج نیازمندی‌های امنیتی و تهدیدهای احتمالی استفاده گردد. عدم توجه به این‌گونه مسائل، صدمه‌های جانی و مالی جبران ناپذیری را برای زندگی انسان‌ها به‌وجود خواهد آورد. روش پیشنهادی با نام ارزیابی امنیتی خودکار مسیرهای تهدید به‌عنوان راه‌حلی برای مقابله با چالش امنیت در فناوری‌های نوظهور

*رایانامه نویسنده مسئول: barzegar@iauns.ac.ir

ناشر: دانشگاه جامع امام حسین (ع)

ارائه‌شده است. در روش ارائه شده، بدون تغییر در فرایندکاری و با اضافه‌کردن قابلیت‌های جدید مانند: احتمال شرطی، امنیت و شی‌گرا به شبکه‌های پتری [۱۳-۱۲-۱۱] که ساده، شبه رسمی و پرکاربرد در مدل‌سازی تهدیدها می‌باشند، یک روش خودکار برای استخراج نیازمندی‌های امنیتی همراه با تولید مسیرهای تهدید، ارزیابی امنیتی کمی و کیفی در مدل‌های تهدید با مقیاس بزرگ ارائه داده است. روش پیشنهادی تمام احتمال‌های ممکن برای یک مدل تهدید را به‌صورت خودکار مورد ارزیابی قرار می‌دهد و مسیرهای امن، ناامن و تهدید را با احتمال نشان خواهد داد.

باقیمانده این مقاله به‌شرح زیر است: بخش ۲ خلاصه‌ای از کارهای مرتبط را نشان می‌دهد، بخش ۳ روش پیشنهادی را توصیف می‌کند. بخش ۴ شبیه‌سازی و ارزیابی مبتنی بر سناریوهای مختلف امنیتی می‌باشد. بخش ۵ بحث و مقایسه با روش‌های موجود و سرانجام، بخش ۶ نتیجه‌گیری مقاله می‌باشد.

۲- کارهای مرتبط

در این بخش، روش‌های مدل‌سازی تهدید خودکار/دستی، مدل سازی رسمی/گرافیکی شرح داده می‌شود. و در پایان، خلاصه‌ای از کارهای انجام شده در مدل‌سازی تهدید و مروری بر شبکه‌های پتری نشان‌داده می شود.

۲-۱- مدل‌سازی خودکار/دستی در مدل‌های تهدید

در مدل‌سازی خودکار، ایکس یو و همکاران [۱۱] رویکردی برای تولید خودکار آزمون‌های امنیتی با استفاده از مدل‌های تهدید رسمی ارائه کرده‌اند اما روش آنها در آزمون‌هایی که بدون شکست یا استثنا اجرا می‌شوند نیازمند تحلیل دستی می‌باشد. علاوه بر این، آرساک و همکاران [۱۴] از مدل چکر برای اعتبارسنجی پروتکل‌های تحت تهدیدهای جدید استفاده کرده‌اند به‌طوری‌که حملات انتقام‌جویانه و قابل پیش‌بینی به‌طور خودکار یافت می‌شوند با این حال، مدل تهدید پیشنهادی آنها هنوز به‌صورت دستی کار می‌کند. در مطالعه دیگری [۱۵]، نویسندگان از ابزار مدل‌سازی تهدید SDL مایکروسافت استفاده کرده‌اند. این ابزار به تجزیه و تحلیل خودکار تهدیدات امنیتی سیستم کمک می‌کند و می‌تواند توسط دیاگرام‌های جریان داده (DFDs) نشان داده شود. اگرچه، روند مدل‌سازی هنوز دستی باقی مانده است. ماسمان و ترنر [۱۶] از الگوریتم‌های بازی امنیت سایبری استفاده کردند که، قابلیت چند سطح خبرگی مانند ترکیب حوادث احتمالی، کشف مسیرهای حمله و تحلیل نمونه کارها را به‌طور خودکار انجام می‌دهد به‌طوری‌که تحلیل‌گران به‌صورت دستی انجام ندهند. از نظر روش‌های مدل‌سازی تهدید، بیشتر مطالعات بر روی مدل‌سازی دستی تمرکز دارند [۱۷]. این نشان می‌دهد که، بیشتر کارهای مدل‌سازی تهدید باقی‌مانده به‌صورت دستی انجام می‌شوند که می‌تواند بسیار وقت‌گیر و مستعد خطا باشد [۱۹-۱۸]. بنابراین، خودکارسازی در مدل‌سازی سیستم‌ها در حال فراگیر شدن می‌باشد.

۲-۲- مدل‌سازی رسمی/گرافیکی در مدل‌های تهدید

روش‌های مدل‌سازی تهدید می‌توانند رسمی/گرافیکی یا ترکیبی از این دو روش باشند. مدل‌سازی رسمی روشی مبتنی بر مدل‌های ریاضی می‌باشد و مدل‌سازی گرافیکی می‌تواند درخت حمله، گراف‌های حمله و جداول باشد [۱۷]. در میان مقاله‌هایی که از مدل‌سازی گرافیکی استفاده کرده‌اند، نویسندگان [۲۱-۲۰] به ترتیب، از درخت‌های حمله برای نشان‌دادن رفتارهای سرقت انرژی در زیرساخت‌های اندازه‌گیری هوشمند (AMI) و تجزیه و تحلیل حملات به سیستم‌های ثبت سلامت الکترونیکی (EHRs) استفاده کرده‌اند، درحالی‌که، الملهم [۲۲] از درخت‌های تهدید به‌منظور تجزیه و تحلیل و برشمردن تهدیدهای تاثیرگذار بر معماری هواپیماهای بدون سرنشین (IoD) استفاده کرده است. علاوه بر این، پی و همکاران [۲۳] از جداول و درخت شکست برای ترسیم چارچوب دفاعی استفاده کرده‌اند که، در روش پیشنهادی آنها از تلفیق تکنیک‌های رمزنگاری، تشخیص ناهنجاری آماری و بررسی نحوی پروتکل برای ساخت مکانیسم‌های دفاعی استفاده شده است. لی یو و همکاران [۲۴] برخی از مدل‌های حمله، جریان‌های اطلاعاتی هدفمند، مکان‌های رخ داده و تکنیک‌های حمله را در یک متر هوشمند مدل کرده‌اند. علاوه بر این، اسلیم و همکاران [۵] از روش جدول تهدید برای طبقه‌بندی تهدیدهای سیستم‌های حمل و نقل هوشمند استفاده شده است. رویکرد جدول تهدید توسط [۲۵] معرفی شد که به‌هیچ‌گونه یادگیری رسمی یا ابزار رسمی احتیاج نداشت. علاوه بر این، در مقایسه با روش‌های رسمی ساده‌تر کار می‌کرد. بدی و همکاران [۲۶] برای ارائه مدل سه مرحله‌ای از مدل STRIDE (شناسایی کلاهبرداری، دستکاری داده، انکار، افشای اطلاعات، انکار سرویس و ارتقا امتیاز) و دارایی‌های بیان شده در جدول تهدید استفاده کرده‌اند. یک رویکرد ماژولار توسط [۲۷] معرفی شد که از هر دو روش مدل‌سازی رسمی و گرافیکی با وزن‌های مختلف استفاده شده است و این نشان می‌دهد که شکل مدل‌سازی تهدید می‌تواند انعطاف پذیر باشد.

جدول (۱) خلاصه‌ای از مطالعه‌های انجام شده در زمینه مدل‌سازی تهدید را ارائه می‌دهد. در این جدول مطالعه‌ها از نظر روش‌های مدل‌سازی (خودکار/دستی و رسمی/گرافیکی) مقایسه شده است.

جدول (۱): خلاصه‌ای از مطالعه‌ها در مدل‌های تهدید

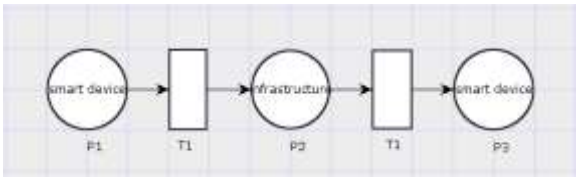
مراجع	رویکرد	روش‌های مدل‌سازی تهدید			
		دستی	خودکار	رسمی	گرافیکی
[۱۱]	با استفاده از شبکه‌های پتری، رویکرد تهدید رسمی را ارائه کردند	✓	✓	✓	✓
[۲۸]	با استفاده از کتابخانه‌های تهدید و طبقه‌بندی تهدیدها، رویکرد طبقه‌بندی تهدید مبتنی بر الگوی دو سطحی را ارائه کردند.	✓	×	✓	✓
[۲۰]	با استفاده از درخت‌های حمله، رویکردی برای تشخیص سرقت انرژی ارائه کردند.	✓	×	✓	✓
[۱۶]	با استفاده از گیم تئوری، روشی برای امتیاز دهی ریسک ارائه کرده‌اند.	×	✓	✓	✓
[۲۴]	با استفاده از شبکه‌های پتری رنگی، رویکردی برای تکنیک‌های طبقه‌بندی حمله ارائه کرده‌اند.	✓	×	×	✓
[۲۹]	با استفاده از سیستم‌های هانی پات، تمام تهدیدهای‌احتمالی را ارائه می‌کند.	✓	×	×	✓
[۳۰]	با استفاده از شبکه‌های پتری جنبه‌گرا، رویکرد تهدید محور رسمی را ارائه کردند.	✓	×	✓	✓
[۳۱]	با استفاده از مدل تهدید STRIDE و رتبه‌بندی ریسک،طبقه‌بندی تهدید و رتبه‌بندی ریسک را ارائه کردند.	✓	×	×	✓

ادامه جدول (۱): خلاصه‌ای از مطالعه‌ها در مدل‌های تهدید

[۳۲]	با استفاده از شبکه‌های پتری، رویکردی برای ادغام شبکه‌های پتری در سیستم گرید ارائه کردند.	✓	×	✓	✓
[۳۳]	با استفاده از متدولوژی رتبه بندی ریسک، چارچوب امنیتی ارائه کردند	✓	×	×	✓
[۳۴]	با استفاده از مدلSTRIDE ، روشی برای ارزیابی درجه امنیت ارائه کرده‌اند.	✓	×	✓	✓
[۳۵]	با استفاده از DFD ، روشی برای کمک به زندگی در محیط هوشمند و نیز ارزیابی ریسک‌های احتمالی ارائه کرده‌اند.	✓	×	×	✓
[۳۶]	با استفاده از DFD ، مشاور خبره امنیتی خودکار را ارائه کردند.	×	✓	✓	✓

۲-۳- مروری بر شبکه‌های پتری

شبکه‌های پتری یک ابزار گرافیکی مبتنی بر نظریه گراف می‌باشد که برای توصیف رسمی از سیستم‌هایی که شامل مجموعه‌ای از رخدادهای گسسته و پراکنده مانند: همزمانی و تعارض، ترتیب‌ها، شاخه‌های شرطی، چرخه‌ها و همگام‌سازی هستند، مورد استفاده قرار می‌گیرد. در یک مدل PNs، مکان (Place) بصورت دایره که حالت سیستم را نشان می‌دهد و گذار (Transition) به‌صورت نوار میله‌ای که رویدادهای تغییر حالت سیستم را نشان می‌دهد و کمان (Arc) ارتباط بین حالت‌های سیستم را نمایش می‌دهد. نشانه (Token) برای بیان وضعیت فعلی شبکه‌های پتری در مکان‌ها قرار می‌گیرد. پس از فعال شدن گذارها، شلیک به‌صورت خودکار انجام می‌شود. شکل (۱) یک مدل مبتنی بر شبکه‌های پتری را نشان می‌دهد. در این شکل، سه مکان (P1,P2,P3) نشان‌دهنده سیستم‌ها (دستگاه‌های هوشمند و زیرساخت) و دو گذار (T1,T2) نشان‌دهنده رویدادهای تغییر حالت سیستم‌ها می‌باشد. نشانه در P1 قرار می‌گیرد.



شکل (۱): مدل مبتنی بر شبکه‌های پتری

برای ارزیابی مدل‌های تهدید، نویسندگان [۳۲- ۳۰- ۲۴- ۱۱] از شبکه‌های پتری برای ارزیابی امنیت سیستم یا تحلیل پروتکل‌های امنیتی استفاده کرده‌اند.

با گسترش حمله‌های سایبری به زیرساخت‌های نظامی و غیرنظامی، پیامدهای ناگواری ایجاد خواهد شد. مدل‌سازی حمله‌های سایبری به تحلیل‌گران امنیتی در ارزیابی اثر حمله‌ها و دفاع پیش‌گیرانه کمک موثری خواهد کرد [۳۹].

در پایان، ارائه یک شبیه‌ساز ارزیابی امنیتی خودکار از مدل‌های تهدید همراه با تضمین امنیتی در سیستم‌های مبتنی بر اینترنت اشیا یک ضرورت مهم و اساسی است.

۳- روش پیشنهادی

ایده اصلی در روش پیشنهادی این است که، به‌منظور کاهش خطا، هزینه، زمان و بررسی حمله‌ها یا تهدیدهای احتمالی بیشتر در آزمون و ارزیابی های مکرر در مدل‌سازی تهدید، در فاز تحلیل و طراحی سیستم‌ها یا توسعه برنامه‌های کاربردی امن، دستیار امنیتی خودکار برای تحلیل‌گران امنیتی ارائه گردد. در این رویکرد، ابتدا مدل پایه امنیتی به نام شبکه‌های پتری شی‌گرا امنیتی (SOOPN) معرفی می‌گردد. مدل پایه امنیتی یک مدل توسعه‌یافته از شبکه‌های پتری می‌باشد که با اضافه‌شدن قابلیت‌های جدید مانند: مفاهیم امنیتی، احتمال شرطی و شی‌گرا [۳۷] به شبکه‌های پتری این مدل تعریف می‌گردد. در روش پیشنهادی بدون تغییر یا دستکاری در روندکاری شبکه‌های پتری، مدل تهدید جدید معرفی شده است. در مدل پایه امنیتی، از مفاهیم امنیتی امن (بدون آسیب پذیری)، ناامن (با آسیب پذیری‌های پرخطر) و تهدید (با آسیب پذیری‌های کم‌خطر) به ترتیب برای نشان‌دادن وضعیت‌های دفاع، حمله و تهدید در حالت‌های مختلف یک سیستم در مدل تهدید جدید می‌باشد و احتمال شرطی (مقادیر بین ۰ و ۱) به عنوان مقادیر احتمالی توسط تحلیل‌گر امنیتی براساس خبرگی، سیاست‌های امنیتی، دفاعی و میزان تهدیدها و آسیب پذیری‌ها در تعیین وضعیتهای یک سیستم استفاده می‌شود. بعد از معرفی مدل پایه امنیتی، الگوریتم‌های تولید خودکار گراف دسترسی، مسیرهای تهدید و احتمال شرطی پیاده‌سازی می‌شود. الگوریتم گراف‌های دسترسی از نود آغازین (ریشه) به نودهای پایانی (برگ) می‌باشد و الگوریتم مسیرهای تهدید، وضعیت‌های نود (امن، ناامن و تهدید) در مسیرهای دسترسی را نشان می‌دهد و در پایان، احتمال شرطی، محاسبه احتمال وضعیت هر نود در مسیرهای دسترسی را نشان خواهد داد.

اهمیت روش پیشنهادی این است که تحلیل‌گر امنیتی می‌تواند سناریوهای مختلف امنیتی را در کمترین زمان با روشی ساده و تمام خودکار با کمک مدل پایه امنیتی طراحی، سنجش و ارزیابی نماید. همچنین هر نوع مولفه سخت‌افزاری یا نرم‌افزاری را با کمترین هزینه و بدون خطا همراه با وضعیت‌های مختلف امنیتی در سیستم‌های پیچیده، حساس، گران‌قیمت که امنیت در آنها از اهمیت ویژه‌ای برخوردار می‌باشد، شبیه‌سازی و سنجش نماید. روش پیشنهادی در شکل (۲) نشان‌داده شده است.

شکل (۲): روش پیشنهادی

۳-۱- پیاده‌سازی الگوریتم شبکه‌های پتری شی‌گرا امنیتی (SOOPN)

در روش پیشنهادی، به‌منظور تعیین وضعیت‌های هر نود در مدل پایه امنیتی، جدول ماتریس وضعیت‌های امنیتی تعریف می‌گردد (جدول ۲ مشاهده شود). بعد از تعیین وضعیت، نتیجه جدید به گذار همان مکان منتقل می‌شود و داده جدید گذار به عنوان ورودی برای نشانه مکان بعدی خواهد بود. این فرایند تا رسیدن به نود پایانی (برگ) در هر مسیر دسترسی ادامه خواهد داشت. در روش پیشنهادی، خروجی ترکیب وضعیت ناامن با دو وضعیت امن یا تهدید، وضعیت ناامن خواهد بود و ترکیب وضعیت امن با تهدید، وضعیت تهدید حاصل می‌شود و فقط ترکیب دو وضعیت امن با امن، نتیجه امن ایجاد خواهد شد. در روش ارائه‌شده خروجی هرترکیب که به گذار آن نود منتقل می‌شود با کمک احتمال شرطی قابلیت کنترل برای شلیک‌شدن آن گذار ایجاد

خواهد شد. این نوع ترکیب اختیاری و قابلیت تغییر دارد. در روش پیشنهادی، نودهای پایانی (برگ) به‌دلیل نداشتن گذار، نتیجه حاصل از ترکیب نشانه و مکان به گذار فرضی با همان شماره نود انتساب داده خواهد شد.

جدول(۲): ماتریس وضعیت‌های امنیتی

		Token		
		Secure(S)	Threat(T)	Insecure(I)
Place	Secure(S)	Secure(S)	Threat(T)	Insecure(I)
	Threat(T)	Threat(T)	Threat(T)	Insecure(I)
	Insecure(I)	Insecure(I)	Insecure(I)	Insecure(I)

در الگوریتم ۱، با استفاده از مفاهیم وراثت [۳۸]، کلاس پایه امنیت (شبه کد ۱) همراه با دو عضو مفاهیم امنیت (شبه کدهای ۲ و ۳) و احتمال شرطی (شبه کدهای ۴ و ۵) در مرحله نخست تعریف می‌گردد. در مرحله بعد، کلاس مکان (شبه کد ۶)، کلاس گذار (شبه کد ۱۱) و کلاس نشانه (شبه کد ۱۳)، کلاس پایه امنیت را به ارث می‌برند. در ادامه، به‌منظور بهره‌مندی از قابلیت گراف شبکه‌های پتری، دو عضو جدید به نام والد (شبه کدهای ۷ و ۸) و فرزند (شبه کدهای ۹ و ۱۰) به کلاس مکان اضافه می‌گردد که از این دو عضو به ترتیب برای نگهداری نود قبلی و نود بعدی استفاده می‌شود. همواره در مدل پایه امنیتی پیشنهادی، والد نود آغازین (ریشه) و فرزند نود پایانی (برگ) NULL می‌باشد و در سایر حالت‌ها، در نودهای میانی، دارای مقادیر خواهد بود. برای کلاس گذار (شبه کد ۱۲) و کلاس نشانه (شبه کد ۱۴) دو عضو والد و فرزند مانند کلاس مکان تعریف می‌شود.

الگوریتم (۱): الگوریتم شبکه‌های پتری شی‌گرا امنیتی

```
Input: Place, Token, Transition, Security concept
Output: Security Object Oriented Petri Nets
(SOOPN)
      // base class
1:    public class Security
       {
2:        public string Security concept
3:            { get; set; }//secure, threat, insecure
4:        public double conditional probability
5:            { get; set;}// (0,1)
      }// end base class
  // derived class: place inherits the members in security
6:        public class Place: Security
              {
                // Properties
7:                public string parent
8:                        { get; set; }
9:                public string child
10:                       { get; set; }
              } //end place
          // Transition inherits the members in security
11:       public class Transition: Security
12:           {  // repeat lines 7-10 } //end Transition
            // Token inherits the members in security
13:         public class Token: Security
14:             {  // repeat lines 7-10 } //end Token
    // end derived class
```

۳-۲- پیاده‌سازی الگوریتم گراف دسترسی و مسیرهای تهدید

با استفاده از گراف دسترسی (الگوریتم ۲ مشاهده شود)، تمام مسیرهای دسترسی از ریشه به برگ قابل دستیابی خواهد بود. در روش ارائه‌شده، پدر در نود ریشه (نود آغازین) و فرزند در نود برگ (نود پایانی) همواره NULL می‌باشد. در مدل پایه امنیتی جدید، به ازای هر مکان ریشه یک مسیر جدید تولید خواهد شد. در الگوریتم ۲، ابتدا دو متغیر پشته و آبجکت تعریف می‌شود (شبه کدهای ۱ و ۲). در ادامه، به ازای هر مکان ریشه دستورات داخل حلقه اجرا خواهد شد (شبه کد ۳)، در داخل حلقه، شرط ریشه بودن مکان بررسی و در صورت درستی شرط (شبه کد ۴)، مکان به پشته اضافه می‌شود (شبه کد ۵). سپس، تازمانی‌که پشته خالی نشده باشد، دستور داخل حلقه while تکرار می‌شود (شبه کد ۶). در داخل حلقه، عنصر بالای پشته از پشته حذف و به متغیر آبجکت انتساب داده می‌شود (شبه کد ۷)، آنگاه شرط مکان بودن یا گذار بودن بررسی می‌گردد (شبه کد ۸ و ۱۲). اگر عنصر مکان باشد در داخل حلقه دو شرط نود پایانی (برگ) یا مکان متصل به گذارها بررسی می‌شود در صورت درستی یکی از شرط‌ها، حلقه اجرا می‌گردد (شبه کد ۹) و تمام گذارهای متصل به آن مکان با شرط NULL نبودن (شبه کدهای ۱۰ و ۱۱) به پشته اضافه می‌گردد. در غیر این صورت (شبه کد ۱۲)، اگر عنصر گذار باشد در داخل حلقه دو شرط نود پایانی (برگ) یا گذار متصل به مکان‌ها بررسی می‌شود در صورت درستی یکی از شرط‌ها، حلقه اجرا می‌گردد (شبه کد ۱۳) و تمام مکان‌های متصل به آن گذار با شرط NULL نبودن (شبه کدهای ۱۴ و ۱۵) به پشته اضافه می‌گردد. این دستور در داخل حلقه while تا رسیدن به برگ ادامه دارد. همان‌طور که گفته شد، در مدل پایه امنیتی به‌دلیل قابلیت شی‌گرا، لیستی از نودها با ویژگی‌هایی مانند: یک نود با والد یکسان و فرزندان متفاوت یا یک فرزند با والد متفاوت (یک مکان با چند گذار مختلف یا یک گذار با چند مکان مختلف) در کنش‌های ترتیبی، همزمان، غیرهمزمان، همگام و همروند ایجاد خواهد شد. به منظور جلوگیری از حلقه بی پایان، تکرارها در داخل لیست قابل شناسایی و حذف خواهد بود.

الگوریتم (۲): الگوریتم تولید خودکار گراف دسترسی

```
Input: threat net as soopn
Output: reachability graph as soopn
1:    Stack<object> stack = new Stack<object> ();
2:    object _object;

3:  foreach ( place is root)
    {
4:     if (root.Parent == "NULL")
        {
5:       stack.Push(place);

6:       while (stack! = null)
          {
7:           _object = stack.Pop();
8:           if (_object is Place)
              {

9:               foreach ((place to transition) or (place to null))
                  {
10:                   if (transition not null)
11:                       stack.Push(transition);
                  }//end foreach
             }//end if
12:          else if (_object is Transition)
              {
13:             foreach ((transition to place) or (transition to null))
                 {
                    //if (place not null)
14:                   if (place not null)
15:                      stack.Push(place);
                 }//end foreach
              } //end else if
          }//end while
       }//end if
                              }//end foreach
```

الگوریتم (۳): الگوریتم تولید خودکار مسیرهای تهدید

```
Input: the list of threat net as soopn
Output: threat paths as soopn – the list of all threat paths
1:  foreach ( place is root )
    {
2:      if (place.Parent is null )
        {
3:       str = string.Empty;
4:       str += token.Security + place.Security;
         //call fillchild(soopn)
5:       FillChild(token , place);

      }//end if
   }//end foreach
    //definition fillchild()
6: private void FillChild(soopn token , soopn p)
    {


7:    foreach (soopn t in ((place to transition) or (transition to
place)
      or (place to null) or (transition to null)))

      {
8:      if (t.Parent == p.Child && p.Child!="NULL")
         {
           // Automated Path Generation
9:          str += "->" + token.Security + t.Security;
10:         FillChild(token , t);
         }//end if
      }//end foreach
   }//end Fill Child
```

۳-۳- پیاده‌سازی الگوریتم تولید خودکار احتمال شرطی

روش محاسبه احتمال شرطی (مقادیر بین ۰ و ۱) که به‌عنوان کلاس پایه در شبکه‌های پتری شی‌گرا امنیتی تعریف شده‌است در جدول (۳) و الگوریتم (۴) نشان داده شده است.

هنگامی‌که دو پیشامد به یکدیگر وابسته باشند و وقوع یا عدم وقوع یکی بر وقوع یا عدم وقوع دیگری تاثیری می‌گذارد، در این صورت وقوع یکی را پس از این‌که دیگری به وقوع پیوسته باشد، محاسبه می‌نمایند چنین احتمالی را احتمال شرطی (قانون ضرب احتمال) می‌گویند. وقوع حادثه A ، به شرط آن‌که بدانیم B رخ داده است به‌صورت P(A|B) نشان داده می‌شود. در روش ارائه‌شده، رفتار نشانه و مکان به‌صورت مستقل فرض شده است. قوانین ضرب احتمال در جدول (۳) نشان داده شده است.

در روش پیشنهادی، ابتدا شرط وضعیت امن، ناامن یا تهدید بودن مکان و نشانه بررسی می‌شود. اگر مکان و نشانه هردو امن باشند خروجی وضعیت آن نود، امن خواهد بود در غیر این‌صورت اگر مکان یا نشانه هر کدام امن نباشد نتیجه وضعیت، ناامن یا تهدید می‌باشد.

این شرایط برای تمامی حالت‌ها از ریشه تا برگ قابل محاسبه و تکرار خواهد بود.

جدول(۳): ماتریس احتمال شرطی

		Token		
		Secure	Threat	Insecure
Place	Secure	احتمال A به شرط B : **$P(A \cap B) = P(A\|B)P(B);$** احتمال B به شرط A : **$P(A \cap B) = P(B\|A)P(A);$** اگر A و B مستقل باشند: **$P(A \cap B) = P(A\|B)P(B) = P(B\|A)P(A) = P(B)P(A) = P(A)P(B);$** مکمل احتمال وقوع حادثه A به شرط وقوع حادثه B : **$P(A'\|B) = 1 - P(A\|B);$**		
	Threat			
	Insecure			

در الگوریتم ۴، تمام حالت‌های قرار گرفتن یک نود در مدل تهدید بررسی می‌شود اگر نود یک مکان ریشه باشد (شبه کد ۱) دستورات داخل این شرط اجرا می‌شود. در داخل شرط، ابتدا، شرط امن بودن مکان و نشانه بررسی می‌شود در صورت درستی شرط مطابق جدول (۳) نتیجه احتمال شرطی به گذار همان نود انتساب داده می‌شود (شبه کدهای ۲، ۳، ۴) در غیراین‌صورت، نتایج دیگر احتمال شرطی مطابق جدول (۳) به گذار انتساب داده می‌شود (شبه کدهای ۵، ۶، ۷). در ادامه، شرط شلیک شدن گذار بررسی و کنترل می‌شود، در صورت امن بودن گذار یا وضعیت تهدید با مقدار احتمالی (a) معین، اجازه شلیک‌شدن به گذار داده

می‌شود. در غیر این صورت، عمل شلیک انجام نمی‌شود (شبه کدهای ۸، ۹، ۱۰، ۱۱). انتخاب شرایط شلیک در روش پیشنهادی قابل تغییر می‌باشد. در سایر حالت‌های قرار گرفتن نود (یک گذار متصل به مکان یا یک مکان متصل به گذار یا یک مکان پایانی) مطابق دستورات بیان شده (از شبه کدهای ۲ تا ۱۱) عمل خواهد شد (شبه کدهای ۱۲، ۱۳، ۱۴).

الگوریتم (۴): الگوریتم تولید خودکار احتمال شرطی

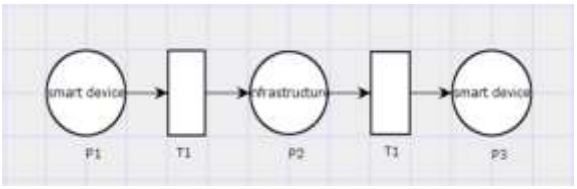
```
Input: Place and Token as soopn
Output: Transition as soopn
1:      if ( Place is root )
         {
           //start calculations code
2:           if (token == secure   and  place == secure)
3:           transition [conditional probability] =
4:           P(A ∩ B) = P(A)P(B);
5:           else if (token! = secure   or place! =secure)
6:                   transition [conditional probability] =
7:             P(A′∩B′) = P(A′)P(B′);
8:           if ((transition == secure)   or  (transition == threat
and
9:           probability < a))
10:          transition can be fired
11:          else transition can not be fired
          //end calculations code
         }//end if
12:     else if (Transition to Place)
              {
               // repeat calculation code:  lines 2-7
              }//end else if
13:     else if (Place to Transition)
              {// repeat calculation code:  lines 2-7
               }//end else if
14:     else if Place is leaf
              {// repeat calculation code:  lines 2-7
              }//end else if
```

۴- ارزیابی

در این بخش، روش ارائه‌شده مبتنی بر سناریوهای مختلف امنیتی شبیه‌سازی و ارزیابی می‌شود. در یک سناریوی فرضی مبتنی بر اینترنت اشیا، دو دستگاه هوشمند از طریق زیرساخت اینترنت اشیا با یکدیگر تعامل دارند. در این سناریو، برای دستگاه‌های هوشمند و زیرساخت وضعیت‌های متفاوتی از امن، تهدید و ناامن در نظر گرفته شده است. در این سناریو، دستگاه هوشمند ۱ داده‌ای را با استفاده از زیرساخت اینترنت اشیا به دستگاه هوشمند ۲ ارسال می‌کند. نشانه در این سناریو نشان‌دهنده وضعیت داده در هر مکان می‌باشد. در روش پیشنهادی در همه سناریوها، نشانه آغازین با احتمال ۰/۷ امن می‌باشد.

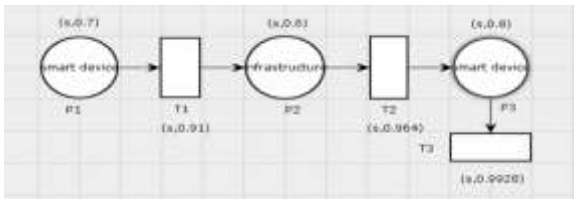
سناریو ۱:

دستگاه هوشمند ۱ و ۲ به‌ترتیب با احتمال ۰/۷ و ۰/۸ امن و زیرساخت با احتمال ۰/۶ در وضعیت امن قرار دارد. مدل تهدید مبتنی برشبکه‌های پتری و شبکه‌های پتری شی‌گرا امنیتی در شکل (۳ و ۴) نشان داده شده است.



شکل(۳): مدل تهدید ۱ مبتنی بر شبکه‌های پتری

نتایج ارزیابی امنیتی خودکار شامل وضعیت گذارها (مقدار احتمال شرطی و وضعیت امنیتی) در شکل (۴) و حالت های قرار گرفتن یک نود در مدل تهدید (نود ریشه، نود میانی یا نود پایانی) با توجه به داده‌های والد و فرزند در آن نود، دنباله‌ای از گراف دسترسی و مسیرهای تهدید با احتمال شرطی مطابق با الگوریتم‌های ارائه شده برای هر نود در جدول (۴) نشان‌داده شده است. این نتایج برای هرنود، از ریشه تا برگ به‌صورت خودکار تولید شده است.



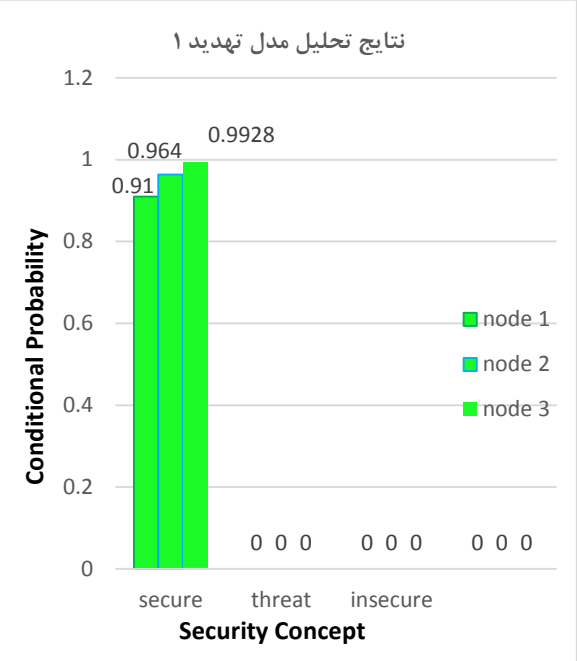
شکل(۴): مدل تهدید ۱ مبتنی بر SOOPN

در جدول (۴)، والد (Parent) و فرزند (Child) نشان‌دهنده حالت‌های قرارگرفتن یک نود در مدل تهدید ۱ می‌باشد. به‌عنوان مثال NULLP1 نود ریشه و P3NULL نود برگ را نشان می‌دهد و سایر حالت ها (به‌عنوان مثال P1T1) نشان‌دهنده نودهای میانی می‌باشد. گراف دسترسی نشان‌دهنده دنباله‌ای از نودهاست (به‌عنوان مثال NULLP1->P1T1) که با استفاده از الگوریتم گراف دسترسی تولید شده است. مسیرهای تهدید نشان‌دهنده دنباله‌ای از وضعیت‌های امنیتی نودها می‌باشد (به‌عنوان مثال SS->SS) که با استفاده از الگوریتم مسیرهای تهدید تولید شده است. احتمال شرطی نشان‌دهنده احتمال وضعیت نشانه و مکان در آن نود می‌باشد که نتیجه حاصل به احتمال گذار آن نود انتساب داده می‌شود (به‌عنوان مثال ۰/۹۱).

جدول(۴): نتایج آزمون خودکار مدل تهدید ۱

Parent	Child	Reachability graph	Threat paths	Threat probability	
NULL	P1	NULLP1	SS	۰/۳ × ۰/۳	۰/۰۹
P1	T1	NULLP1->P1T1	SS->SS	۱ -۰/۰۹	۰/۹۱
T1	P2	NULLP1->P1T1->T1P2	SS->SS->SS	۰/۰۹ × ۰/۴	۰/۰۳۶
P2	T2	NULLP1->P1T1->T1P2->P2T2	SS->SS->SS->SS	۱ -۰/۰۳۶	۰/۹۶۴
T2	P3	NULLP1->P1T1->T1P2->P2T2->T2P3	SS->SS->SS->SS->SS	۰/۰۳۶× ۰/۲	۰/۰۰۷۲
P3	NULL	NULLP1->P1T1->T1P2->P2T2->T2P3->P3NULL	SS->SS->SS->SS->SS->SS	۱ -۰/۰۰۷۲	۰/۹۹۲۸

نتایج، مسیر امن را نشان می‌دهد. داده‌های تولید شده در جدول (۴) به منظور تحلیل در شکل (۵) استفاده می‌شود.

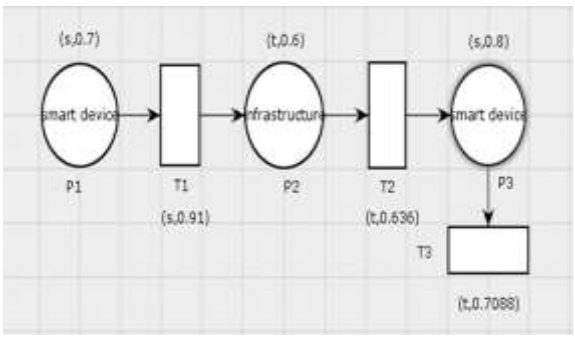


شکل(۵): نتایج تحلیل مدل تهدید ۱

نتایج به‌دست آمده از آزمون مدل تهدید در شکل (۵) نشان داده شده است. این شکل مفاهیم امنیتی (امن، تهدید و ناامن) را در محور افقی و احتمال شرطی (مقادیر بین ۰ و ۱) را در محور عمودی نشان می‌دهد. وضعیت هر نود سطح امنیت مولفه سخت افزاری یا نرم افزاری را نشان می‌دهد.

سناریو۲:

دستگاه هوشمند ۱ و ۲ به ترتیب با احتمال ۰/۷ و ۰/۸ امن و زیرساخت با احتمال ۰/۶ در وضعیت تهدید قرار دارد. مدل تهدید مبتنی بر شبکه‌های پتری شی‌گرا امنیتی در شکل (۶) نشان داده شده است.



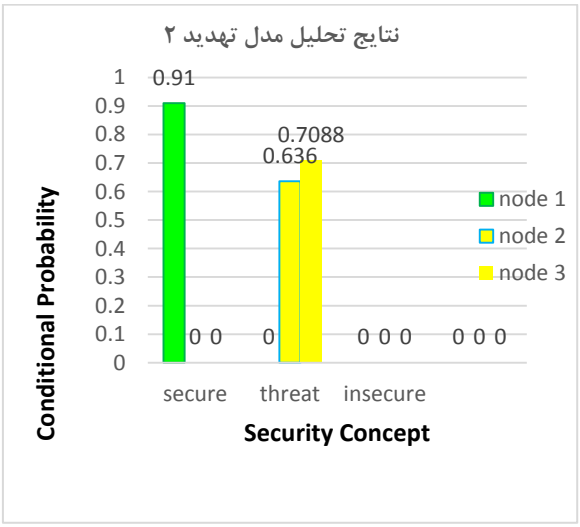
شکل(۶): مدل تهدید ۲ مبتنی بر SOOPN

نتایج ارزیابی امنیتی خودکار سناریو ۲ در جدول (۵) و شکل (۶) نشان داده شده است.

جدول(۵): نتایج آزمون خودکار مدل تهدید ۲

Parent	Child	Reachability graph	Threat paths	Threat probability	
NULL	P1	NULLP1	SS	۰/۳ × ۰/۳	۰/۰۹
P1	T1	NULLP1->P1T1	SS->SS	۱ -۰/۰۹	۰/۹۱
T1	P2	NULLP1->P1T1->T1P2	SS->SS->ST	۰/۹۱ × ۰/۴	۰/۳۶۴
P2	T2	NULLP1->P1T1->T1P2->P2T2	SS->SS->ST->TS	۱ -۰/۳۶۴	۰/۶۳۶
T2	P3	NULLP1->P1T1->T1P2->P2T2->T2P3	SS->SS->ST->TS->TS	۰/۳۶۴×۰/۸	۰/۲۹۱۲
P3	NULL	NULLP1->P1T1->T1P2->P2T2->T2P3->P3NULL	SS->SS->ST->TS->TS->TS	۱ -۰/۲۹۱۲	۰/۷۰۸۸

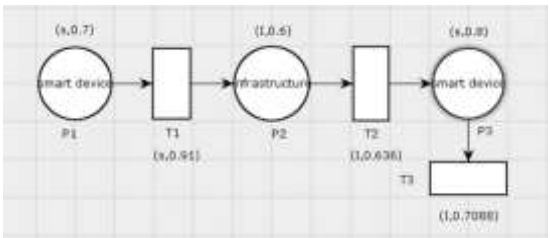
نتایج، مسیری امن همراه با تهدید را نشان می‌دهند. نتایج تحلیل هر مولفه در شکل (۷) نشان داده شده است.



شکل(۷): نتایج تحلیل مدل تهدید ۲

سناریو ۳:

دستگاه هوشمند ۱ و ۲ به ترتیب با احتمال ۰/۷ و ۰/۸ امن و زیرساخت با احتمال ۰/۶ در وضعیت ناامن قرار دارد. مدل تهدید مبتنی شبکه‌های پتری شی‌گرا امنیتی در شکل (۸) نشان داده شده است.



شکل(۸): مدل تهدید ۳ مبتنی بر SOOPN

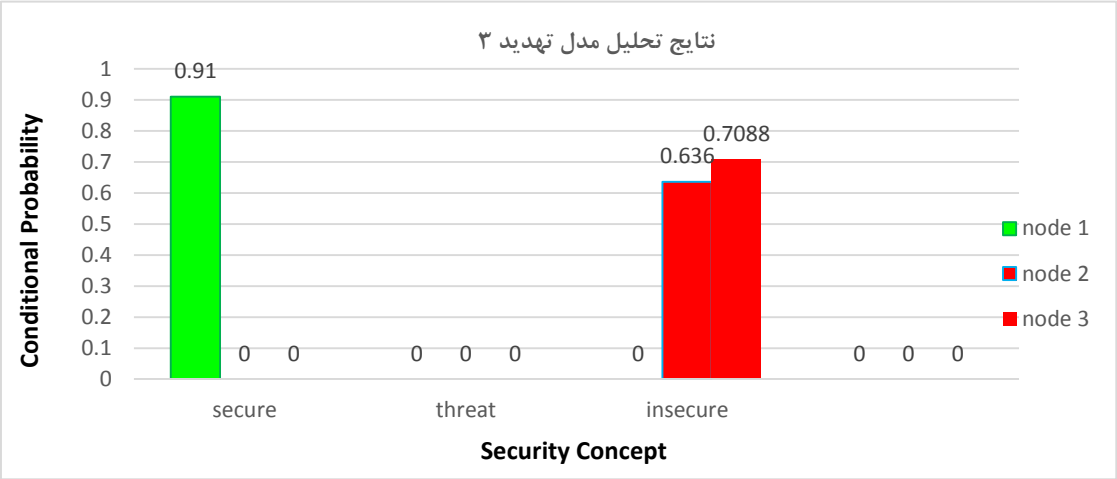
نتایج ارزیابی امنیتی خودکار سناریو ۳ در جدول (۶) و شکل (۸) نشان داده شده است.

نتایج، مسیری امن و ناامن را نشان می‌دهد. نتایج تحلیل هر مولفه در شکل (۹) نشان داده شده است.

به‌منظور ارزیابی بیشتر روش پیشنهادی، جدول (۷) خلاصه‌ای از نتایج آزمون خودکار سناریوهای متفاوت دیگر را نشان می‌دهد.

جدول(۶): نتایج آزمون خودکار مدل تهدید ۳

Parent	Child	Reachability graph	Threat paths	Threat probability	
NULL	P1	NULLP1	SS	۰/۳ × ۰/۳	۰/۰۹
P1	T1	NULLP1->P1T1	SS->SS	۱ -۰/۰۹	۰/۹۱
T1	P2	NULLP1->P1T1->T1P2	SS->SS->SI	۰/۹۱ × ۰/۴	۰/۳۶۴
P2	T2	NULLP1->P1T1->T1P2->P2T2	SS->SS->SI->IS	۱ -۰/۳۶۴	۰/۶۳۶
T2	P3	NULLP1->P1T1->T1P2->P2T2->T2P3	SS->SS->SI->IS->IS	۰/۳۶۴×۰/۸	۰/۲۹۱۲
P3	NULL	NULLP1->P1T1->T1P2->P2T2->T2P3->P3NULL	SS->SS->SI->IS->IS->IS	۱ -۰/۲۹۱۲	۰/۷۰۸۸



شکل(۹): نتایج تحلیل مدل تهدید ۳

جدول (۷): خلاصه‌ای از نتایج سناریوهای بیشتر

سناریو	نتایج آزمون خودکار	دستگاه هوشمند ۲	زیرساخت	دستگاه هوشمند ۱	نشانه آغازین
۴	NULLP1->P1T1->T1P2->P2T2->T2P3->P3NULL SI->SI->II->II->II->II ۰/۷۹->۰/۹۱۶->۰/۹۸۳۲	I	I	I	S
۵	NULLP1->P1T1->T1P2->P2T2->T2P3->P3NULL ST->ST->TT->TT->TT->TT ۰/۷۹->۰/۹۱۶->۰/۹۸۳۲	T	T	T	S
۶	NULLP1->P1T1->T1P2->P2T2->T2P3->P3NULL SS->SS->SI->SI->IT->IT ۰/۹۱->۰/۶۳۶->۰/۹۲۷۲	T	I	S	S
۷	NULLP1->P1T1->T1P2->P2T2->T2P3->P3NULL SI->SI->IT->IT->II->II ۰/۷۹->۰/۹۱۶->۰/۹۸۳۲	I	T	I	S
۸	NULLP1->P1T1->T1P2->P2T2->T2P3->P3NULL SI->SI->IS->IS->II->II ۰/۷۹->۰/۹۱۶->۰/۹۸۳۲	I	S	I	S

۵- بحث

در این بخش، روش پیشنهادی با برخی کارهای موجود از نظر رویکرد (کیفی و کمی)، روش (دستی/خودکار و رسمی/گرافیکی) و روش‌های اعتبارسنجی مورد بحث قرار گرفته است.

طبقه‌بندی تهدیدات به‌عنوان معیار کیفی در مدل‌سازی تهدیدات معرفی می‌شود [۱۷] . روش‌های موجود به دو گروه تهدیدات یا حملات امنیتی عمومی [۳۳ ,۳۰ ,۱۱] و خاص [۲۸, ۲۴, ۲۰] دسته‌بندی می‌شوند. روش پیشنهادی با بهره‌مندی از مدل پایه امنیتی قابلیت پشتیبانی از هر دو گروه طبقه‌بندی تهدیدات امنیتی را دارد.

زمان، هزینه، دقت و احتمال به‌عنوان معیارهای کمی برای مقایسه روش پیشنهادی با سایر روش‌ها ارائه می‌شود. به‌طور قابل اثباتی روش‌های خودکار از منظر سرعت، مقرون به صرفه‌بودن و کاهش خطا بر روش‌های نیمه خودکار [۱۱] و دستی [۳۳ ,۳۰ ,۲۴ ,۲۸ ,۲۰] برتری دارد. الگوریتم تولید مسیر روش پیشنهادی در محیط برنامه‌نویسی سی‌شارپ پیاده‌سازی شده و نتایج آزمون سرعت با ۱۰ نود به‌ترتیب برای ۱ مسیر، ۱۰ مسیر و ۱۰۰ مسیر به ترتیب ۲۴ میلی‌ثانیه، ۱۶۱ میلی‌ثانیه و ۲۸۲ میلی‌ثانیه می‌باشد. در روش دستی در خوش‌بینانه‌ترین حالت، اگر هر نود در ۱۰ ثانیه ارزیابی شود ۱۰ نود در ۱ مسیر در ۱۰۰ ثانیه، ۱۰ مسیر در ۱۰۰۰ ثانیه و ۱۰۰ مسیر در ۱۰۰۰۰۰ ثانیه ارزیابی خواهد شد. همچنین، اگر هزینه تحلیل در ۱ ثانیه ۱ واحد باشد در روش پیشنهادی برای ۱۰۰ مسیر کسری از ۱ واحد هزینه خواهد بود. درحالی‌که، در روش‌های دستی، برای ۱۰۰ مسیر ۱۰۰۰۰۰ واحد هزینه می‌باشد. نتایج نشان می‌دهد، در روش‌های دستی، هرچه تعداد نود و مسیرها افزایش یابد زمان و هزینه به‌صورت نمایی افزایش می‌یابد و این نشان می‌دهد که، روش ارائه‌شده بر سایر روش‌های موجود برتری دارد. در روش پیشنهادی، نتایج به‌دست آمده اثبات کننده این واقعیت است که مدل پایه امنیتی علاوه بر قابلیت‌های خودکار، دارای احتمال تهدید می‌باشد. روش پیشنهادی در مقایسه با روش‌های موجود، تمام احتمال‌های ممکن برای هر نود در یک مسیر را محاسبه خواهد کرد. اگر هر نود دارای سه وضعیت امن، ناامن یا تهدید باشد در نتیجه طبق اصل ضرب از اصول چندگانه شمارش، n نود در یک مسیر دارای 3^n وضعیت خواهد بود که روش پیشنهادی به‌صورت خودکار در کمترین زمان و با کمترین هزینه و بدون خطا تمام مسیرها و احتمالات را تولید خواهد کرد. در مثال ارائه شده، ۲۷ حالت را به‌صورت خودکار برای یک مسیر تولید خواهد کرد.

از منظر روش‌های اعتبارسنجی در مدل‌های تهدید، روش‌های موجود از روش شبیه‌سازی [۲۴]، مثال [۲۸]، مطالعه موردی [۳۳ ,۳۰ ,۱۱]، بدون اعتبارسنجی [۲۰] استفاده شده است. در حالی‌که، روش پیشنهادی دارای شبیه‌ساز خودکار توسعه‌یافته مبتنی بر مدل پایه امنیتی می‌باشد.

جدول (۸) خلاصه‌ای از مقایسه روش پیشنهادی با روش های موجود را از نظر رویکرد و روش نشان می‌دهد.

جدول(۸): مقایسه روش پیشنهادی با روش‌های موجود

مراجع	کیفی	کمی	دستی	خودکار	رسمی	گرافیکی
[۱۱]	تولید تمام مسیرهای حمله	×	✓	✓	✓	✓
[۲۸]	طبقه‌بندی تهدید	×	✓	×	✓	✓
[۲۰]	×	کمینه کردن خطای طبقه‌بندی	✓	×	✓	✓
[۲۴]	×	تکنیک‌های طبقه‌بندی حمله	✓	×	×	✓
[۳۰]	اعتبارسنجی تهدید	×	✓	×	✓	✓
[۳۳]	طبقه‌بندی تهدید	میزان احتمال خطر	✓	×	×	✓
روش پیشنهادی	طبقه‌بندی تهدید و امنیت، تولید تمام خودکار مسیرهای تهدید	میزان احتمال تهدید	×	✓	✓	✓

در پایان، در مقایسه با آخرین روش‌های مدل‌سازی تهدید، روش پیشنهادی از نظر کاهش زمان، هزینه و خطای انسانی به‌دلیل تمام خودکار بودن، بهتر عمل خواهد کرد و تضمین امنیتی سطح بالا را ارائه خواهد داد.

۶- نتیجه‌گیری و کارهای آینده

امنیت چالش اساسی در فناوری‌های جدید می‌باشد که عدم توجه به آن گاهی صدمات جانی و مالی زیان‌باری برای انسان‌ها در زندگی

روزمره ایجاد خواهد کرد. در این مقاله، با معرفی مدل پایه امنیتی، راه‌حلی خودکار با تضمین امنیتی سطح بالا ارائه شده است که تحلیل‌گران امنیتی می‌توانند مکان و چگونگی اعمال ویژگی‌های امنیتی برای کاهش تهدیدات در مدل‌های تهدید مقیاس بزرگ را شناسایی و استخراج نمایند. مدل پایه امنیتی، یک مدل توسعه‌یافته از شبکه‌های پتری می‌باشد که قابلیت‌های جدید مانند: احتمال شرطی، مفاهیم امنیت و شی‌گرا به آن اضافه شده است. روش پیشنهادی، روشی خودکار در تولید مسیرهای دسترسی، مسیرهای تهدید همراه با احتمال را نشان داده است. در ادامه، تولید ابزار کمکی تحلیل‌گران امنیتی مبتنی بر روش پیشنهادی یا ارزیابی اصالت داده در سیستم‌های مبتنی بر اینترنت اشیا، از اهداف آتی خواهد بود.

۷- مراجع

[1] M. Shunmei, G. Zijian, L. Qianmu, W. Hao, D. Hong-Ning and Q. Lianyong, "Security-Driven hybrid collaborative recommendation method for cloud-based iot services," Computers & Security, 2020.

[2] Z. Mahmood, "Connected vehicles in the iov: Concepts, technologies and architectures," In: Connected vehicles in the internet of things : Springer, 2020.

[3] A. Kumar, A. K. Jain and M. Dua, "A comprehensive taxonomy of security and privacy issues in RFID," Complex Intell. Syst., 2021.

[4] G. Tripathi, M. Ahad and M. Sathiyanarayanan, "The role of blockchain in internet of vehicles (iov): Issues, challenges and opportunities," In: 2019 international conference on contemporary computing and informatics (IC3I). IEEE, pp. 26-31, 2019.

[5] L. Sleem, H. N. Noura and R. Couturier, "Towards a secure ITS: Overview, challenges and solutions," Journal of Information Security and Applications, vol. 55, 2020.

[6] M. Zhang, C. Chen, T. Wo, T. Xie, M. Bhuiyan and X. Lin, "Safedrive: online driving anomaly detection from large-scale vehicle data," IEEE Trans Ind Inf, vol. 13, no. 4, pp. 2087-96, 2017.

[7] O. Abu Waraga, M. Bettayeb, Q. Nasir and M. Abu Talib, "Design and Implementation of Automated IoT Security Testbed," Computers & Security, vol. 88, 2020.

[8] B. D. Deebak and F. AL-Turjman, "Secure-user sign-in authentication for IoT-based eHealth systems," Complex Intell. Syst, 2021.

[9] S. Tanwar, K. Parekh and R. Evans, "Blockchain-based electronic healthcare record system for healthcare 4.0 applications," Journal of Information Security and Applications, 2020.

[10] L. Chen , W. Lee , C.-H. Chang, K.-K. Raymond Choo and N. Zhang , "Blockchain based searchable encryption for electronic health record sharing," Fut Gener Comput Syst, vol. 95, pp. 420-9, 2019.

[11] D. Xu, M. Tu, M. Sanford, L. Thomas, D. Woodraska and W. Xu, "Automated Security Test Generation with Formal Threat Models," IEEE Transactions on Dependable and Secure Computing, vol. 9, no. 4, pp. 526-540, 2012.

[12] B. Barzegar and H. Motameni, "Modeling and simulation firewall using Colored Petri Nets," World Appl. Sci. j, vol. 15, no. 6, pp. 826-830, 2011.

[13] B. Barzegar, S. Ghanbari, H. Bozorgi and M. Rahimi, "Modeling and simulation of traffic lights and controller unit systems by Colored Petri Nets," Int. j. Phys. Sci, vol. 6, no. 34, pp. 7760-7770, 2011.

[14] W. Arsac, G. Bella, X. Chantry and L. Compagna, "Multi-Attacker Protocol Validation," Journal of Automated Reasoning, vol. 46, no. 4, pp. 353-388, 2011.

[15] A. O. Baquero, A. J. Kornecki and J. Zalewski, "Threat Modeling for Aviation Computer Security," Fusing IT & Real-Time Tactical, vol. 28, pp. 21-27, 2015.

[16] S. Musman and A. Turner, "A game oriented approach to minimizing cybersecurity risk," International Journal of Safety and Security Engineering, vol. 8, no. 2, pp. 212-222, 2018.

[17] W. Xiong and R. Lagerström, " Threat modeling -- A systematic literature review," Computers & Security, vol. 84, pp. 53-69, 2019.

[18] H. Holm, M. Buschle, R. Lagerstrom and M. Ekstedt, "Automated data collection for enterprise architecture models," Softw syst model, vol. 13, no. 2, p. 825, 2014.

[19] P. Närman, P. Johnson, R. Lagerström, U. Franke and M. Ekstedt, " Data Collection Prioritization for System Quality Analysis," Electronic Notes in Theoretical Computer Science, vol. 233, pp. 29-42, 2009.

[20] R. Jiang, R. Lu, Y. Wang, J. Luo, C. Shen and X. S. Shen, "Energy-Theft Detection Issues for Advanced Metering Infrastructure in Smart Grid," Science and Technology, vol. 19, no. 2, pp. 105-120, 2014.

[21] A. Almulhem, "Threat Modeling for Electronic Health Record Systems," Journal of Medical Systems, vol. 36, no. 5, 2012.

[22] A. Almulhem, "Threat modeling of a multi-UAV system," Transportation Research Part A: policy and practice, pp. 290-295, 2020.

[23] D. Pei, L. Zhang and D. Massey, "A framework for resilient Internet routing protocols," IEEE Network, vol. 18, no. 2, pp. 5-12, 2004.

[24] X. Liu, P. Zhu, Y. Zhang and K. Chen, "A Collaborative Intrusion Detection Mechanism Against False Data Injection Attack in Advanced Metering Infrastructure," IEEE Transactions on Smart Grid, vol. 6, no. 5, pp. 435-443, 2015.

[25] J. C. Pendergrass, K. Heart, C. Ranganathan and V. N. Venkatakrishnan, "A threat table based assessment of information security in telemedicine," International Journal of Healthcare Information Systems and Informatics, vol. 9, no. 4, pp. 20-31, 2014.

Modeling of Obfuscated Multi-Stage Cyber Attacks," Journal of Electronical & Cyber Defence, vol. 8, no. 2, p. 61, 2020, (In Persion).

[26] P. Bedi, V. Gandotra, A. Singhal, H. Narang and S. Sharma, "Threat-oriented security framework in risk management using multiagent system," Software:P ractice and Experience, vol. 43, pp. 1013-1038, 2013.

[27] G. Brændeland, A. Refsdal and K. Stølen, "Modular analysis and modelling of risk scenarios with dependencies," The Journal of Systems & Software, vol. 83, no. 10, pp. 1995-2013, 2010.

[28] A. V. Uzunov and E. B. Fernandez,, "An extensible pattern-based library and taxonomy of security threats for distributed systems," Computer Standards & Interfaces, vol. 36, no. 4, pp. 734-747, 2014.

[29] R. N. Dahbul, C. Lim and J. Purnama, "Enhancing Honeypot Deception Capability Through Network Service Fingerprinting," Journal of Physics:Conference Series, pp. 1-6, 2017.

[30] D. Xu and K. E. Nygard, "Threat-Driven Modeling and Verification of Secure Software Using Aspect-Oriented Petri Nets," IEEE Transactions on Software Engineering, vol. 32, no. 4, pp. 265-278, 2006.

[31] D. Seifert and H. Reza, "A Security Analysis of Cyber-Physical Systems Architecture for Healthcare," Computers, vol. 5, no. 27, pp. 1-24, 2016.

[32] M. Kalinin and A. Konoplev, "Formalization of objectives of grid systems resources protection against unauthorized access," Nonlinear Phenomena in Complex Systems, vol. 17, no. 3, pp. 272-277, 2014.

[33] J. Meszaros and A. Buchalcevova, "Introducing OSSF: A framework for online service cybersecurity risk management," Computers & Security, vol. 65, pp. 300-313, 2017.

[34] X. Chen, Y. Liu and J. Yi, "A Security Evaluation Framework Based on STRIDE Model for Software in Networks," International Journal of Advancements in Computing Technology, vol. 4, no. 13, pp. 269-278, 2012.

[35] V. Olawumi, K. Haataja and P. Toivanen, "Security Issues in Smart Homes and Mobile Health System: Threat Analysis, Possible Countermeasures and Lessons Learned," International Journal on Information Technologies & Security, vol. 9, no. 1, p. 31, 2017.

[36] M. Frydman, G. Ruiz, E. Heymann, E. César and B. P. Miller, "Automating Risk Analysis of Software Design Models," The Scientific World Journal, pp. 1-12, 2014.

[37] Microsoft, "object-oriented programing," Microsoft, 2020. [Online]. Available: https://docs.microsoft.com/en-us/dotnet/csharp/tutorials/intro-to-csharp/object-oriented-programming.

[38] Microsoft, "Inheritance," Microsoft, 2020. [Online]. Available: https://docs.microsoft.com/en-us/dotnet/csharp/programming-guide/classes-and-structs/inheritance.

[39] K. Shoushian, A. J. Rashidi and A. R. Mirghadri, "Probabilistic