**Passive Defence**

Vol. 16, No. 3, Autumn 2025, Serial No. 63

**ISSN: 2980-8030 , E-ISSN: 2008-6849**

# Reducing Cyber Risks in the Internet of Things Using Hybrid Graph and Behavioral Deep Learning Models

**Afshar Khosravi[1*], Mohammad Ali Javadzadeh[2]**

[1]Correspondence: Ph.D. Student in Computer Engineering, University of Imam Hossein, Tehran, Iran. Email Address: khosravi_afshar@ihu.ac.ir

[2]Assistant Professor of Computer Science, University of Imam Hossein, Tehran, Iran. Email Address: javadzadeh@ihu.ac.ir

ARTICLE INFO

***Article history:***

Article Type: Research paper

Received: 24 November 2024

Received in revised form: 18 May 2025

Accepted: 20 September 2025

Available online: 22 October 2025

***Keywords:***

Cyber Risk Reduction

Internet of Things (IoT)

Behavioral Analysis

Graph Neural Networks (GNN)

Deep Learning

ABSTRACT

Cybersecurity in the Internet of Things (IoT) is a critical area of information and communication technology that faces major challenges due to the complexity and dynamic nature of IoT systems. One of the primary issues in this domain is the detection of anomalies and sophisticated cyberattacks, which stem from the structural complexity and unpredictable behaviors of interconnected devices. These security threats can severely affect system integrity, performance, and data confidentiality. Previous research has explored various approaches, including temporal behavior analysis and network communication modeling, to mitigate cyber risks. However, when applied independently, these approaches often fail to provide a comprehensive defense mechanism. To address these limitations, this study proposes a hybrid approach that integrates graph-based modeling with behavioral deep learning methods. Specifically, by representing device interactions as graphs and analyzing temporal variations using Graph Neural Networks (GNNs) and Long Short-Term Memory (LSTM) models, the proposed method enhances anomaly detection and reduces the likelihood of cyberattacks, thereby lowering overall cyber risk. Experimental evaluations conducted on IoT-related datasets demonstrate that the proposed model significantly outperforms conventional methods. The results show superior performance metrics with 0.92 accuracy, 0.91 precision, 0.94 recall, and an F1-score of 0.92, along with a reduced false alarm rate. These findings highlight the effectiveness of the proposed approach in strengthening IoT cybersecurity, representing a significant advancement in risk reduction and system protection.

**Cite this article:** A. Khosravi and M. A. Javadzadeh, "Reducing Cyber Risks in the Internet of Things Using Hybrid Graph and Behavioral Deep Learning Models," Journal of Passive Defence, vol. 16, no. 3, pp. 55-62, 2025. **DOR: 20.1001.1.20086849.1404.16.3.4.2**

**Publisher**: Imam Hossein University.

پدافند غیرعامل

سال پانزدهم، شماره ۳، پاییز ۱۴۰۴، (پیاپی ۶۳): صص ۶۲-۵۵

**شاپای چاپی:** ۶۹۴۹-۲۰۰۸ | **شاپای الکترونیکی:** ۸۰۳۰-۲۹۸۰

# کاهش خطر سایبری اینترنت اشیاء با استفاده از مدل‌های ترکیبی گراف و یادگیری عمیق رفتاری

**افشار خسروی[1*]، محمدعلی جوادزاده[2]**

[1]دانشجوی دکتری کامپیوتر دانشگاه جامع امام حسین(ع)، تهران، ایران. رایانامه: khosravi_afshar@ihu.ac.ir

[2]استادیار کامپیوتر دانشگاه جامع امام حسین(ع)، تهران، ایران. رایانامه: javadzadeh@ihu.ac.ir

## چکیده

امنیت سایبری در اینترنت اشیاء[1] یک حوزه حیاتی در فناوری اطلاعات و ارتباطات است که به دلیل پیچیدگی و ماهیت پویای سامانه‌های اینترنت اشیاء با چالش‌های مهمی مواجه است. یکی از مسائل اولیه در این زمینه، تشخیص ناهنجاری‌ها و حمله‌های سایبری پیچیده است که از پیچیدگی‌های ساختاری و رفتارهای غیرقابل‌پیش‌بینی دستگاه‌های متصل‌به‌هم نشئت می‌گیرد. این تهدیدهای امنیتی می‌توانند به‌شدت بر یکپارچگی سامانه، عملکرد و محرمانه بودن داده‌ها تأثیر بگذارند. تحقیقات قبلی روش‌های مختلفی از جمله تحلیل رفتار زمانی و مدل‌سازی ارتباطات شبکه را برای کاهش خطرهای سایبری، مورد بررسی قرار داده‌اند. بااین‌حال، این رویکردها، زمانی‌که به‌صورت مجزا به کار می‌روند، اغلب در ارائه یک سازوکار دفاعی جامع شکست می‌خورند. برای پرداختن به این محدودیت‌ها، این مطالعه یک رویکرد ترکیبی را پیشنهاد می‌کند که مدل‌سازی مبتنی بر گراف را با روش‌های یادگیری رفتاری عمیق ادغام می‌کند. به طور خاص، با نمایش ارتباطات دستگاه به‌عنوان گراف و تجزیه‌وتحلیل تغییرهای زمانی با استفاده از مدل‌های شبکه‌های عصبی گراف[2] و حافظه کوتاه‌مدت[3]، روش پیشنهادی تشخیص ناهنجاری را افزایش و احتمال حمله‌های سایبری را کاهش داده و در نتیجه خطر کلی سایبری را کاهش می‌دهد. ارزیابی‌های تجربی انجام‌شده بر روی مجموعه‌داده‌های[4] مرتبط با اینترنت اشیاء نشان می‌دهد که مدل پیشنهادی به طور قابل‌توجهی از روش‌های مرسوم بهتر عمل می‌کند. نتایج، نشان‌دهنده معیارهای عملکرد برتر با صحت ۹۲٪، دقت ۰/۹۱، یادآوری ۰/۹۴ و امتیاز F1 ۰/۹۲ در کنار کاهش نرخ هشدار نادرست است. این یافته‌ها بر اثربخشی رویکرد پیشنهادی در تقویت امنیت سایبری اینترنت اشیاء تأکید می‌کند، که نشان‌دهنده پیشرفت قابل‌توجهی در کاهش خطر و افزایش امنیت سامانه است.

## مشخصات مقاله

**تاریخچه مقاله:**

نوع مقاله: علمی پژوهشی

دریافت: ۱۴۰۳/۱۱/۱۴

بازنگری: ۱۴۰۳/۱۲/۱۸

پذیرش: ۱۴۰۴/۰۶/۲۹

ارائه آنلاین: ۱۴۰۴/۰۷/۳۰

**کلیدواژه‌ها:**

کاهش خطر سایبری امنیت

اینترنت اشیاء

تحلیل رفتاری

شبکه‌های عصبی گراف

یادگیری عمیق

[1] Internet of Things
[2] GNN
[3] LSTM
[4] Datasets

**استناد:** خسروی، افشار، جوادزاده، محمدعلی، " کاهش خطر سایبری اینترنت اشیاء با استفاده از مدل‌های ترکیبی گراف و یادگیری عمیق رفتاری"، نشریه پدافند غیرعامل، دوره ۱۶، شماره۳، صفحات ۶۲-۵۵، ۱۴۰۴. DOR: 20.1001.1.20086849.1404.16.3.4.2

**ناشر:** دانشگاه جام امام حسین(ع).

## ۱- مقدمه

اینترنت اشیاء جنبه‌های مختلف زندگی مدرن را با امکان اتصال یکپارچه بین دستگاه‌های مختلف و ادغام آنها با اینترنت متحول کرده است. اینترنت اشیاء با قابلیت‌هایی مانند جمع‌آوری بی‌درنگ داده‌ها، تجزیه‌وتحلیل هوشمند و خودکارسازی فرایند، کارایی و بهره‌وری را در صنایع، زیرساخت‌های حیاتی و زندگی روزمره به طور قابل‌توجهی افزایش داده است. بااین‌حال، با افزایش اتکا به اینترنت اشیاء، چالش‌های امنیت سایبری آن نیز افزایش می‌یابد. پیچیدگی ذاتی معماری‌های اینترنت اشیاء، تعداد زیاد دستگاه‌های متصل‌به‌هم و ناهمگونی پروتکل‌های ارتباطی، این سامانه‌ها را به اهداف اصلی حمله‌های سایبری تبدیل می‌کند. تهدیدهایی مانند آلودگی به بدافزار، حمله‌های منع سرویس توزیع‌شده[1] و نفوذهای غیرمجاز، مخاطره‌های قابل‌توجهی را برای محرمانگی، یکپارچگی و دردسترس‌بودن داده‌ها و زیرساخت‌های حیاتی ایجاد می‌کند [۱].

تشخیص ناهنجاری[2] یک رویکرد کلیدی برای پرداختن به این چالش‌های امنیت سایبری است که سازوکاری مؤثر برای شناسایی انحراف‌ها در رفتار سامانه اینترنت اشیاء ارائه نموده که ممکن است نشان‌دهنده حمله‌های سایبری یا شکست‌های عملیاتی باشد. تشخیص به‌موقع چنین ناهنجاری‌هایی برای جلوگیری از نقض امنیت و به‌حداقل‌رساندن آسیب‌های احتمالی بسیار مهم است. بااین‌حال، روش‌های مرسوم تشخیص ناهنجاری تلاش می‌کنند تا به طور هم‌زمان هم روابط ساختاری و هم تغییرهای زمانی را در داده‌های اینترنت اشیاء ثبت و اثربخشی آنها را محدود کنند. این چالش بر نیاز به روش‌شناسی پیشرفته تأکید کرده که بتواند ساختارهای شبکه پیچیده و الگوهای رفتاری زمانی را در اکوسیستم‌های اینترنت اشیاء مدل‌سازی و تحلیل کند [۲].

برای مقابله با این موضوع، تحقیق‌های ما بر توسعه یک رویکرد جامع و یکپارچه متمرکز است که تشخیص ناهنجاری و کاهش خطر سایبری در سامانه‌های اینترنت اشیاء را افزایش می‌دهد. ما یک روش مبتکرانه مبتنی بر یادگیری عمیق را پیشنهاد می‌کنیم که تجزیه‌وتحلیل شبکه را با مدل‌سازی رفتاری زمانی ترکیب می‌کند. در این چارچوب، داده‌های ارتباطی اینترنت اشیاء به‌عنوان یک گراف شبکه نشان داده می‌شود که در آن از شبکه‌های عصبی گراف برای کشف الگوهای رابطه‌ای پیچیده در بین دستگاه‌های متصل استفاده می‌شود. به طور هم‌زمان، مدل‌های تحلیل زمانی، مانند شبکه‌های حافظه کوتاه‌مدت و معماری‌های ترانسفورمر[1]، برای ثبت تغییرهای پویا در ویژگی‌های داده متوالی استفاده می‌شوند. این رویکرد ترکیبی یک راه‌حل قوی و مقیاس‌پذیر برای شناسایی تهدیدهای سایبری پیچیده، از جمله حمله‌های چندمرحله‌ای و روز صفر ارائه می‌دهد.

هدف اصلی این تحقیق، پیشبرد رویکردهای امنیت سایبری برای سامانه‌های اینترنت اشیاء با ارائه یک سازوکار تشخیص ناهنجاری دقیق و تطبیقی است. با استفاده از روش پیشنهادی، تحلیلگران امنیتی می‌توانند تهدیدها را بادقت بیشتری شناسایی کنند، آسیب‌پذیری‌ها را به طور فعال کاهش داده و انعطاف‌پذیری زیرساخت‌های اینترنت اشیاء را در برابر خطرهای سایبری به طور قابل‌توجهی افزایش دهند.

ساختار این مقاله به صورت زیر تنظیم شده است: در بخش دوم، به بررسی کارهای مرتبط پرداخته می‌شود تا پیشینه تحقیق و مطالعه‌های انجام‌شده در این حوزه مرور گردد. در بخش سوم، روش پیشنهادی ارائه می‌شود و جزئیات رویکرد اتخاذشده توضیح داده می‌شود. در بخش چهارم، نتایج حاصل از آزمایش‌ها و تحلیل‌های انجام‌شده بررسی شده و مورد بحث قرار می‌گیرد. در بخش پنجم، جمع‌بندی نتایج و نتیجه‌گیری کلی ارائه خواهد شد. در نهایت، در بخش ششم، مراجع و منابع مورد استفاده ذکر می‌شوند.

## ۲- کارهای مرتبط

اینترنت اشیاء به دلیل استقرار در مقیاس بزرگ، اکوسیستم دستگاه‌های ناهمگن و اتصال‌های پیچیده، چالش‌های امنیتی متعددی را ارائه می‌دهد. حمله‌های سایبری که سامانه‌های اینترنت اشیاء را هدف قرار می‌دهند، می‌توانند داده‌های حساس و زیرساخت‌های حیاتی را به خطر بیندازند و منجر به خسارت‌های مالی قابل‌توجه و آسیب‌های اعتباری شوند [۳]. در سال‌های اخیر، پیشرفت‌ها در تحلیل رفتار غیرعادی و مدل‌های امنیتی ترکیبی، راه را برای شناسایی تهدید مؤثرتر و رویکردهای کاهش خطر در امنیت اینترنت اشیاء هموار کرده است.

درحالی‌که برنامه‌های کاربردی اینترنت اشیاء مزایای قابل‌توجهی از جمله افزایش بهره‌وری عملیاتی، بهبود راحتی و کیفیت زندگی بهتر برای افراد، کسب و کارها و جامعه ارائه می‌دهند، اما خطرهای امنیت سایبری قابل‌توجهی را نیز به همراه دارند. پذیرش گسترده

[1] DDoS
[2] Anomaly Detection

فناوری‌های اینترنت اشیاء، تعداد سطوح حمله احتمالی را افزایش داده و محیط‌های اینترنت اشیاء را به اهداف جذابی برای عوامل مخرب تبدیل می‌کند. نقض امنیت در سامانه‌های اینترنت اشیاء می‌تواند محرمانه بودن، یکپارچگی و در دسترس بودن داده‌ها را به خطر بیندازد و منجر به آسیب فیزیکی، مالی و اعتباری برای سازمان‌ها و کاربران شود [۴].

برای مقابله با این چالش‌ها، یک چارچوب سیستماتیک امنیت سایبری هنگام طراحی برنامه‌های کاربردی مبتنی بر اینترنت اشیاء ضروری است. چنین چارچوبی باید روش‌های ساختار یافته‌ای را برای شناسایی، ارزیابی و مدیریت خطرهای امنیت سایبری سیستماتیک و در عین حال امکان واکنش سریع به حوادث امنیتی ارائه دهد. یکی از رویکردهای امیدوارکننده، تحلیل رفتار غیرعادی[۲] است که نقش مهمی در شناسایی تهدیدهای سایبری در اکوسیستم‌های اینترنت اشیاء ایفا می‌کند. با تجزیه و تحلیل انحراف‌ها در رفتارهای دستگاه و تعامل‌های شبکه، تحلیل رفتار غیرعادی توانایی شناسایی تهدیدهای امنیتی را به طور فعال افزایش می‌دهد و در نهایت انعطاف پذیری زیرساخت‌های اینترنت اشیاء را تقویت می‌کند [۵].

## ۲-۱- چشم‌انداز اینترنت اشیاء و خطر امنیتی

تحقیق‌ها، چالش‌ها و خطرهای امنیتی متعدد مرتبط با دستگاه‌های اینترنت اشیاء را برجسته نموده که ناشی از عواملی مانند ناهمگونی، مقیاس‌پذیری، کیفیت خدمت‌ها[۳] و الزام‌های امنیتی و مدیریتی متنوع است. این پیچیدگی‌ها، محیط‌های اینترنت اشیاء را در برابر تهدیدهای سایبری بسیار آسیب‌پذیر می‌کند. فقدان معیارهای خطر امنیتی درست تعریف‌شده و بهینه نه تنها احتمال نقض امنیت را افزایش می‌دهد، بلکه بی اعتمادی را در بین ذینفعان تقویت نموده و مانع پذیرش گسترده فناوری‌های اینترنت اشیاء می‌شود [۶].

شکل (۱) یک نمای کلی از چالش‌های امنیتی کلیدی در اکوسیستم اینترنت اشیاء و خطرهای چندوجهی را نشان می‌دهد که باید برای اطمینان از یک زیرساخت امن و انعطاف‌پذیر اینترنت اشیاء مورد توجه قرار گیرند.

[1] Transformer
[2] Anomaly Behaviour Analysis
[3] QoS


**شکل (۱)**: چالش‌های اینترنت اشیاء[۴] (ناهمگونی[۵]، تشخیص ناهنجاری[۶]، پیش‌بینی خطر امنیتی[۷]، کیفیت خدمات[۸]، مدیریت داده[۹]، مقیاس‌پذیری[۱۰])[۶]

## ۲-۲- اینترنت اشیاء و ناهنجاری‌های امنیتی

در یک سامانه اینترنت اشیاء، حسگرها به طور مداوم شرایط دنیای فیزیکی را بررسی و اندازه‌گیری می‌کنند. در شرایط عادی، داده‌کاوی و کشف دانش اغلب به دلیل فقدان اطلاعات اضافی یا غیرمنتظره، بینش قابل‌توجهی ایجاد نمی‌کنند. با این حال، زمانی‌که داده‌های حسگر[۱۱] رفتار غیرعادی از خود نشان می‌دهند، می‌توانند رویدادهای حیاتی مانند شناسایی تقلب در کارت اعتباری، وخامت شرایط سلامت، نقص عملکرد دستگاه، تشخیص سرقت و سایر حوادث مرتبط با امنیت را نشان دهند [۷].

تشخیص ناهنجاری برای اطمینان از حریم خصوصی داده‌ها، امنیت و پیش‌بینی خطر سایبری در محیط‌های اینترنت اشیاء ضروری است. انحراف در داده‌های حسگر می‌تواند نشانه‌ای از خطاها، خرابی‌های سامانه، حمله‌های سایبری یا رویدادهای نادری باشد که نیاز به توجه فوری دارند. زمینه‌های مختلف، از جمله مدیریت خطر، تشخیص تقلب و تصمیم‌گیری، برای جلوگیری از نقض امنیت، کاهش تقلب و افزایش اطلاعات عملیاتی بر تشخیص ناهنجاری تکیه دارند [۸].

[4] IoT Challenges
[5] Heterogeneity
[6] Anomaly Detection
[7] Predict Security Risk
[8] Quality of Service
[9] Data Management
[10] Scalability
[11] Sensor

داده‌های حساس و محافظت‌نشده ممکن است حاوی اطلاعات مهمی باشند که در صورت به‌خطرافتادن، می‌تواند منجر به خطرهای امنیتی جدی شود. ناهنجاری‌ها از منابع مختلفی مانند خطاهای سامانه، حمله‌های خارجی، خرابی‌های سخت‌افزاری یا رویدادهای نادر اما مهم ناشی می‌شوند. شناسایی و تجزیه و تحلیل این ناهنجاری‌ها برای کاهش پیشگیرانه خطر بسیار مهم است. به طور کلی، ناهنجاری‌ها به سه نوع طبقه‌بندی می‌شوند [۹-۱۱]:

۱. ناهنجاری‌های نقطه: انحراف در یک نقطه داده فردی.
۲. ناهنجاری‌های زمینه‌ای: انحراف‌هایی‌که در یک محیط خاص رخ می‌دهند.
۳. ناهنجاری‌های جمعی: انحراف‌های مشاهده‌شده در کل مجموعه‌داده یا سامانه [۱۲-۱۴].

تشخیص ناهنجاری و امتیازدهی جمعی نقش کلیدی در بهبود روش‌های ارزیابی خطر، به‌ویژه در افزایش محاسبه‌های ارزش سایبری در معرض خطر[1] ایفا می‌کند، زیرا نمره‌های ناهنجاری فردی اغلب دارای تناقض هستند [۱۵].

روش‌های سنتی تجزیه و تحلیل خطر به دلیل تکامل سریع الگوهای داده و رفتارهای سامانه برای امنیت اینترنت اشیاء ناکافی هستند. تحلیلگران مرکز عملیات امنیتی[2] اغلب بر اساس اطلاعات قدیمی و تحت تأثیر عدم قطعیت‌های داخلی و خارجی تصمیم می‌گیرند. برای مقابله با این چالش‌ها، شناسایی ناهنجاری‌ها در داده‌های اینترنت اشیاء در مقیاس بزرگ، استخراج متغیرهای پویا از رویدادهای غیرعادی و ادغام مداوم آنها در موتورهای ارزیابی خطر ضروری است. این رویکرد با تطبیق با تهدیدهای امنیتی بلادرنگ، پیش‌بینی خطر دقیق‌تری را ممکن می‌سازد.

شکل (۲) رویکرد مدل‌سازی مبتنی بر ACP را نشان می‌دهد که تحلیل‌های پیش‌بینی‌کننده[3]، تجویزی[4] و توصیفی[5] را برای تحلیل خطر سایبری پیشگیرانه تسهیل می‌کند. با استفاده از چارچوب‌های پیشرفته تشخیص ناهنجاری، می‌توان امنیت اینترنت اشیاء را به میزان قابل‌توجهی افزایش داد و از وضعیت امنیت سایبری انعطاف‌پذیرتر و سازگارتر اطمینان داد [۱۶].

[1] Cyber Value at Risk
[2] SOC (Security Operation Center)
[3] Predictive
[4] Perspective
[5] Prescribe


**شکل (۲):** جریان محاسبه خطر اینترنت اشیاء[6] [۱۶]

## ۳-روش پیشنهادی

این مطالعه با هدف پاسخگویی به این سؤال تحقیق انجام می‌شود که چگونه می‌توان خطرهای امنیت سایبری اینترنت اشیاء را با شناسایی و تجزیه و تحلیل ناهنجاری‌های پیچیده در رفتار دستگاه و تعامل‌های شبکه به طور موثر کاهش داد؟

برای پرداختن به این چالش، ما چارچوب جدیدی پیشنهاد می‌شود که تجزیه و تحلیل ساختاری مبتنی بر گراف را با یادگیری عمیق رفتاری زمانی ادغام می‌کند تا تشخیص ناهنجاری و کاهش خطر امنیت سایبری در سامانه‌های اینترنت اشیاء را افزایش دهد. رویکرد پیشنهادی شامل اجزای کلیدی زیر است:

### ۳-۱- تجزیه و تحلیل ساختاری مبتنی بر گراف

در اینجا هدف مدل‌سازی و تجزیه و تحلیل روابط بین دستگاه‌های اینترنت اشیاء، آدرس‌های IP و پروتکل‌های ارتباطی به عنوان یک گراف شبکه برای شناسایی الگوهای تعامل غیرعادی است.

برای این موضوع، یک گراف شبکه ساخته می‌شود که در آن گره‌ها دستگاه‌های اینترنت اشیاء یا آدرس‌های IP و لبه‌ها نشان دهنده اتصال‌های ترافیکی یا پروتکل‌های ارتباطی هستند. از شبکه‌های عصبی گراف برای استخراج ویژگی‌های گراف، از جمله درجه گره، ضرایب خوشه‌بندی و معیارهای کوتاه‌ترین مسیر استفاده می‌شود. شناسایی ناهنجاری‌های ساختاری، مانند اتصال‌های مشکوک و الگوهای فعالیت مخرب در شبکه است.

[6] IoT Risk Calculation Flow:Risk Calculation & Mitigation, IoT System, Anomaly Detection, Anamalous Event Analysis, Dynamic Variables Extraction, Validation with Static Information

### ۳-۲-تجزیه و تحلیل رفتار زمانی با استفاده از حافظه کوتاه‌مدت و ترانسفورماتور

هدف، شناسایی الگوهای غیرمعمول در داده‌های زمانی اینترنت اشیاء، مانند تغییرها در شدت حمله یا انحراف‌ها در رفتار دستگاه در طول زمان است. بدین منظور، یک مدل مبتنی بر حافظه کوتاه‌مدت برای تجزیه و تحلیل ویژگی‌های سری زمانی، از جمله مُهرهای‌زمانی[1]، طول بسته‌ها و الگوهای تکرار رویداد ایجاد می‌شود. یک مدل ترانسفورماتور را نیز برای گرفتن وابستگی‌های دوربرد و بهبود تشخیص ناهنجاری‌های رفتاری پیچیده و پویا ادغام می‌شود.

### ۳-۳- ادغام مدل‌های ساختاری و زمانی

برای افزایش دقت تشخیص ناهنجاری، ویژگی‌های ساختاری مبتنی بر گراف را با ویژگی‌های رفتاری زمانی در یک لایه کاملاً متصل ادغام می‌کنیم. لایه خروجی نهایی (لایه متراکم) احتمال ناهنجاری را پیش‌بینی و ناهنجاری‌های شناسایی‌شده را بر اساس الگوهای آموخته‌شده طبقه‌بندی می‌کند.

### ۳-۴- ارزیابی خطر با استفاده از ارزش سایبری در معرض خطر

برای تعیین کمیت تأثیر ناهنجاری‌های شناسایی‌شده، ما از ارزش سایبری در معرض خطر به عنوان معیاری برای ارزیابی خطر سایبری استفاده می‌کنیم. ارزش سایبری در معرض خطر با یکپارچه‌سازی محاسبه می‌شود [۱۵]:

- نمره‌های ناهنجاری تجمعی از مدل‌های ساختاری و زمانی.
- مقادیر دارایی دستگاه‌های تحت تأثیر برای تعیین بحرانی بودن آنها.

عوامل خطر متنی، امکان اولویت‌بندی تطبیقی رویکردهای کاهش خطر سایبری را فراهم می‌کند.

### ۳-۵- مقیاس پذیری و اجرای بلادرنگ

برای اطمینان از کاربرد این چارچوب در محیط‌های بی‌درنگ اینترنت اشیاء، استخراج ویژگی‌های کارآمد و روش‌های پردازش مقیاس‌پذیر را برای مدیریت جریان‌های داده اینترنت اشیاء با حجم بالا و سرعت بالا ترکیب می‌کنیم. این بهینه‌سازی تشخیص ناهنجاری و ارزیابی خطر را در زمان واقعی امکان‌پذیر می‌سازد و از نظارت امنیتی قوی در اکوسیستم‌های پویا اینترنت اشیاء اطمینان حاصل می‌کند.

### ۳-۶- مشارکت‌های مورد انتظار

چارچوب پیشنهادی با هدف ارائه چندین کمک کلیدی به امنیت سایبری اینترنت اشیاء است:

- **تشخیص ناهنجاری بهبود یافته:** رویکرد ترکیبی با ادغام تجزیه و تحلیل شبکه ساختاری با مدل‌سازی رفتاری زمانی، تشخیص تهدیدهای پیچیده از جمله حمله‌های چند مرحله‌ای و آسیب‌پذیری‌های روز صفر را افزایش می‌دهد.
- **کاهش مثبت کاذب۲: با ترکیب الگوریتم‌های مکمل، این چارچوب هشدارهای کاذب را کاهش می‌دهد و از تشخیص دقیق‌تر و مطمئن‌تر تهدید اطمینان می‌دهد.**
- **بینش خطر عملیاتی: ادغام ارزش سایبری در معرض خطر به سا**زمان‌ها این امکان را می‌دهد که به طور سیستماتیک خطرهای امنیت سایبری را ارزیابی و اولویت‌بندی کنند و تصمیم گیری را برای کاهش خطر بهبود بخشند.

### ۳-۷- مراحل پیاده‌سازی

برای پیاده‌سازی چارچوب پیشنهادی، ادغام تجزیه و تحلیل گراف با استفاده از شبکه عصبی گراف و تحلیل زمانی با استفاده از حافظه کوتاه‌مدت در مراحل زیر انجام می‌شود:

**مرحله ۱: پیش‌پردازش داده‌ها**

در ابتدا گراف‌های شبکه را از آدرس‌های IP، پروتکل‌های ارتباطی و داده‌های ترافیک استخراج می‌کنیم. سپس، داده‌های سری زمانی پردازش می‌شود. در اینجا ویژگی‌هایی مانند مهرزمانی، طول بسته‌ها و فرکانس‌های رویداد استخراج می‌شود تا تجزیه و تحلیل متوالی را فعال نماید. در این مرحله داده‌های دارای مقدار نامشخص[3] از مجموعه‌داده انتخابی حذف و فرمت‌های مهرزمانی به داده‌های عددی قابل پردازش تبدیل می‌شوند و بعد دسته‌بندی ترافیک به عادی[4] و حمله[5] با استفاده از ستون "Action Taken" انجام می‌گردد.

[1] Timestamps

[2] False Positive
[3] Missing Values
[4] Normal
[5] Attack

**مرحله ۲: طراحی مدل**

در اینجا یک شبکه عصبی گراف برای تجزیه و تحلیل گراف شبکه طراحی شده و ویژگی‌های ساختاری مانند درجه گره، ضرایب خوشه‌بندی و کوتاه‌ترین مسیرها استخراج می‌شود. سپس یک مدل یادگیری عمیق مبتنی بر حافظه کوتاه‌مدت برای تجزیه و تحلیل داده‌های زمانی و شناسایی الگوهای رفتاری پویا در ترافیک اینترنت اشیاء ایجاد می‌کنیم. در انتها خروجی شبکه عصبی گراف (ویژگی‌های ساختاری) را با خروجی حافظه کوتاه‌مدت (ویژگی‌های زمانی) در یک شبکه کاملاً متصل و به دنبال آن یک لایه متراکم نهایی برای پیش‌بینی احتمال‌های ناهنجاری را ادغام می‌کنیم. در واقع برای تحلیل ساختاری، ارتباط بین آدرس‌های IP به گراف شبکه تبدیل و از شبکه عصبی گراف برای تحلیل روابط استفاده می‌شود. برای تحلیل زمانی و رفتاری، ویژگی‌های مربوط به زمان‌بندی، طول بسته‌ها و نرخ ارسال داده‌ها به عنوان ورودی به حافظه کوتاه‌مدت/ترانسفرومر داده می‌شود تا تغییرات غیرعادی تشخیص داده شوند.

**مرحله ۳: ارزیابی مدل**

داده‌ها به دو بخش آموزش (۸۰٪) و آزمایش (۲۰٪) تقسیم می‌شوند. مدل پیشنهادی را در برابر روش‌های تشخیص ناهنجاری سنتی با اندازه‌گیری معیارهای کلیدی مانند دقت، امتیاز F1 و نرخ هشدار نادرست ارزیابی می‌کنیم. همچنین ارزیابی اثربخشی چارچوب در تشخیص ناهنجاری‌های پیچیده و کاهش خطرهای سایبری در سامانه‌های اینترنت اشیاء را انجام می‌دهیم.

## ۳-۸- ابزارها و فناوری‌ها

برای توسعه و ارزیابی چارچوب، از ابزارها و فناوری‌های زیر استفاده می‌کنیم:

تجزیه و تحلیل گراف شبکه: ساخت و تجزیه و تحلیل گراف با استفاده از NetworkX یا PyTorch Geometric پیاده‌سازی شده است.

مدل‌های یادگیری عمیق: با استفاده از PyTorch یا TensorFlow برای تشخیص ناهنجاری مبتنی بر شبکه عصبی گراف و حافظه کوتاه‌مدت توسعه یافته است.

معیارهای ارزیابی: معیارهای استاندارد یادگیری ماشین مانند امتیاز F1، دقت[1]، یادآوری[2] و نرخ هشدار کاذب برای ارزیابی عملکرد مدل استفاده می‌شوند.

## ۳-۹- مجموعه‌داده

مجموعه‌داده مورد استفاده در این مطالعه از Kaggle [۱۷]، به طور خاص یک مجموعه‌داده سایبری مصنوعی تولیدشده توسط Incribo به دست آمده است. این مجموعه‌داده شامل اطلاعات مربوط به امنیت سایبری در دستگاه‌های اینترنت اشیاء، شبکه‌ها و رویدادهای امنیتی است. تشخیص الگو، تحلیل روند و ارزیابی خطر را تسهیل می‌کند.

### ۳-۹-۱- ویژگی‌های کلیدی مجموعه‌داده:

- تعداد کل ویژگی‌ها: ۲۵
- تعداد رکوردها: ۴۰،۰۰۰
- نوع داده‌ها: شامل ویژگی‌های ساختاری[3]، زمانی[4] و رفتاری[5].
- نوع حمله‌ها: این مجموعه داده شامل ترافیک عادی و حمله‌های سایبری مختلف، از جمله منع‌سرویس توزیع‌شده، Brute Force، بدافزار[6] و اسکن شبکه[7] است.

### ۳-۹-۲- ویژگی‌های مهم مجموعه‌داده

- آدرس‌های IP مبدا و مقصد
- پروتکل ارتباطی
- طول بسته‌های ارسالی و دریافتی
- زمان‌بندی رویدادها
- نوع حمله یا عادی بودن ترافیک

این مجموعه‌داده برای ارزیابی مدل‌های تشخیص ناهنجاری در محیط‌های اینترنت اشیاء، حصول اطمینان از آزمایش واقع‌بینانه و اعتبارسنجی چارچوب پیشنهادی مناسب است.

## ۴- نتایج و بحث

در این قسمت نتایج بدست آمده از روش پیشنهادی و سایر روش‌ها از مقاله‌های مرتبط در یک جدول مقایسه می‌شود. این جدول شامل معیارهای ارزیابی صحت[8]، امتیاز F1، دقت[9] و یادآوری و روش‌های استفاده‌شده است.

[1] Precision
[2] Recall
[3] Graph-based
[4] Temporal
[5] Behavioral
[6] Malware
[7] Network Scaning
[8] Accuracy
[9] Precision

| مقاله | روش | صحت | دقت | امتیاز F1 |
|---|---|---|---|---|
| [۵] | Anomaly Behavior Analysis (ABA) | ٪۸۷ | ٪۸۴ | ٪۸۵ |
| [۷] | IoT Healthcare Anomaly Detection | ٪۸۹ | ٪۸۷ | ٪۸۸ |
| [۸] | ML-Enabled Anomaly Detection | ٪۹۰ | ٪۸۸ | ٪۸۹ |
| [۹] | Supervised Machine Learning | ٪۸۸ | ٪۸۵ | ٪۸۶ |
| **روش پیشنهادی** | GNN + LSTM | **٪۹۲** | **٪۹۰** | **٪۹۲** |

**جدول (۱):** مقایسه پارامترهای ارزیابی

چارچوب ترکیبی پیشنهادی، که شبکه‌های عصبی گراف را برای تجزیه و تحلیل ساختار شبکه و حافظه کوتاه‌مدت برای مدل‌سازی رفتار زمانی ادغام می‌کند، به صحت ۹۲ درصد فراتر از رویکردهای سنتی دست می‌یابد. این قابلیت افزایش یافته، شناسایی تهدیدهای سایبری پیچیده، از جمله حمله‌های چند مرحله‌ای و سوء استفاده‌های روز صفر را ممکن می‌سازد.

در مقایسه با روش‌های قبلی، مدل پیشنهادی عملکرد بهتری از نظر صحت، دقت و امتیاز F1 نشان داده است. این بهبود به دلیل ترکیب مدل‌سازی ساختاری (شبکه عصبی گراف) و تحلیل زمانی(حافظه کوتاه مدت) است که باعث می‌شود حملات پیچیده و چندمرحله‌ای با دقت بیشتری شناسایی شوند.

در مقابل، روش‌های سنتی مانند ABA ([۵]) و یادگیری نظارت‌شده ([۹]) قادر به درک همزمان ساختار شبکه و الگوهای زمانی نیستند، که دقت و صحت آن‌ها را کاهش می‌دهد. علاوه بر این، روش‌های جدیدتری مانند ترانسفورمرهای سری زمانی و اتوانکودرها[1] نیز مطرح شده‌اند. ترانسفورمرها توانایی یادگیری الگوهای پیچیده را دارند، اما در تحلیل ارتباطات شبکه به خوبی شبکه عصبی گراف عمل نمی‌کنند. از سوی دیگر، اتوانکودرها می‌توانند ناهنجاری‌های کلی را شناسایی کنند اما نسبت به حملات چندمرحله‌ای حساسیت کافی ندارند.

اگرچه مدل پیشنهادی عملکرد بهتری دارد، اما چالش‌هایی مانند پیچیدگی محاسباتی و نیاز به داده‌های برچسب‌دار وجود دارد. در تحقیقات آینده، استفاده از یادگیری نیمه‌نظارت‌شده یا یادگیری تطبیقی می‌تواند به بهبود تعمیم‌پذیری مدل کمک کند.

در ادامه مقایسه با روش‌های موجود، مزایای رویکرد ما را برجسته می‌کند:

روش [۵]: برای تجزیه و تحلیل رفتارهای غیرعادی مؤثر است، اما فاقد توانایی مدل‌سازی همزمان ساختارهای شبکه و وابستگی‌های زمانی است که دقت تشخیص کلی آن را محدود می‌کند.

روش [۷]: متخصص در امنیت اینترنت اشیاء در سامانه‌های مراقبت‌های بهداشتی، نشان دادن عملکرد قوی در آن حوزه. با این حال، به خوبی به محیط‌های مختلف اینترنت اشیاء تعمیم نمی‌یابد.

روش [۸]: از تشخیص ناهنجاری مبتنی بر یادگیری ماشین استفاده می‌کند، که به خوبی عمل می‌کند، اما روابط پیچیده شبکه را مدل نمی‌کند و اثربخشی آن را در برابر الگوهای حمله پیچیده کاهش می‌دهد.

روش [۹]: از یادگیری نظارت‌شده استفاده می‌کند که به شدت به کیفیت و حجم داده‌های برچسب گذاری‌شده وابسته است. در حالی‌که در مجموعه‌داده‌های دارای حاشیه‌نویسی مناسب مؤثر است، در سناریوهای اینترنت اشیاء در دنیای واقعی که داده‌های برچسب‌گذاری‌شده اغلب کمیاب هستند، با مشکل مواجه می‌شود.

با ادغام تجزیه و تحلیل شبکه مبتنی بر گراف با تشخیص ناهنجاری زمانی، رویکرد پیشنهادی از روش‌های قبلی در معیارهای ارزیابی کلیدی بهتر عمل می‌کند و راه‌حلی جامع و قوی برای امنیت سایبری اینترنت اشیاء ارائه می‌دهد. در جدول (۲)، مقایسه در یک نگاه روش‌های سنتی با روش پیشنهادی آورده شده است:

**جدول (۲):** مقایسه پارامترهای روش‌های سنتی و روش پیشنهادی

| مقاله | روش | مدل‌سازی روابط بین دستگاه‌های اینترنت اشیاء | تحلیل الگوهای زمانی | تشخیص حملات پیچیده چندمرحله‌ای | مقیاس پذیری به حوزه‌های مختلف اینترنت اشیاء |
|---|---|---|---|---|---|
| [۵] | Anomaly Behavior Analysis (ABA) | □ ندارد | □ دارد اما محدود | □ ضعیف در شناسایی حملات چندمرحله‌ای | □ خیر |
| [۷] | IoT Healthcare Anomaly Detection | □ بله اما خاص به یک حوزه | □ ندارد | □ خیر | □ فقط برای IoT پزشکی |
| [۸] | ML-Enabled Anomaly Detection | □ ندارد | □ دارد اما ساده | □ خیر | □ بله اما دقت پایین |
| [۹] | Supervised Machine Learning | □ محدود | □ دارد | □ نیازمند داده‌های زیاد | □ خیر |
| **روش پیشنهادی** | GNN + LSTM | □ بله، شبکه عصبی گراف روابط گرافی را مدل‌سازی می‌کند | □ بله، LSTM وابستگی‌های زمانی را تحلیل می‌کند | □ بله، حملات چندمرحله‌ای را بهتر شناسایی می‌کند | □ بله، در حوزه‌های مختلف اینتر اشیاء قابل استفاده است |

[1] Autoencoder

## ۵- نتیجه گیری

این مقاله یک رویکرد ترکیبی جدید مبتنی بر شبکه‌های عصبی گراف و حافظه کوتاه‌مدت برای شناسایی تهدیدات سایبری در سامانه‌های اینترنت اشیاء ارائه می‌کند. برخلاف روش‌های قبلی که تنها یکی از این دو جنبه را در نظر می‌گرفتند، مدل پیشنهادی ساختار شبکه را مدل‌سازی کرده و هم‌زمان الگوهای زمانی را تحلیل می‌کند. این ترکیب منحصربه‌فرد باعث شده است که دقت تشخیص بهبود یابد، نرخ مثبت کاذب کاهش یابد و حملات پیچیده و چندمرحله‌ای بهتر شناسایی شوند.

علاوه بر این، مقایسه با روش‌های موجود نشان می‌دهد که بیشتر تحقیقات پیشین یا صرفاً به روابط بین دستگاه‌های اینترنت اشیاء پرداخته‌اند یا فقط بر تحلیل زمانی متمرکز بوده‌اند. روش پیشنهادی، با ادغام این دو رویکرد، برای اولین بار تشخیص تهدیدهای چندمرحله‌ای را در محیط‌های مختلف اینترنت اشیاء بهبود می‌بخشد.

با این وجود، برخی چالش‌ها مانند پیچیدگی محاسباتی و نیاز به داده‌های برچسب‌دار وجود دارد که در آینده می‌توان با استفاده از مدل‌های بهینه‌سازی‌شده و یادگیری نیمه‌نظارت‌شده آن‌ها را بهبود داد. این رویکرد می‌تواند به‌طور گسترده در حوزه‌های مختلف مانند خانه‌های هوشمند، صنعت و حمل‌ونقل هوشمند برای بهبود امنیت سایبری اینترنت اشیاء مورد استفاده قرار گیرد.

## ۶- مراجع


[1] R. Kaur, D. Gabrijelčič, and T. Klobučar, "Artificial intelligence for cybersecurity: Literature review and future research directions," Information Fusion, vol. 97, p. 101804, 2023.

[2] Z. Liu, Y. Zhou, Y. Xu, and Z. Wang, "Simplenet: A simple network for image anomaly detection and localization," in Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, 2023, pp. 20402-20411 .

[3] A.-A. Bouramdane, "Cyberattacks in smart grids: challenges and solving the multi-criteria decision-making for cybersecurity options, including ones that incorporate artificial intelligence, using an analytical hierarchy process," Journal of Cybersecurity and Privacy, vol. 3, no. 4, pp. 662-705, 2023.

[4] M. Elsisi, M. Altius, S.-F. Su, and C.-L .Su, "Robust Kalman filter for position estimation of automated guided vehicles under cyberattacks," IEEE Transactions on Instrumentation and Measurement, vol. 72, pp. 1-12, 2023.

[5] J. Pacheco, X. Zhu, Y. Badr, and S. Hariri, "Enabling risk management for smart infrastructures with an anomaly behavior analysis intrusion detection system," in 2017 IEEE 2nd International Workshops on Foundations and Applications of Self* Systems (FAS* W), 2017: IEEE, pp. 324-328 .

[6] N. Mishra and S. Pandya, "Internet of things applications, security challenges, attacks, intrusion detection, and future visions: A systematic review," IEEE Access, vol. 9, pp. 59353-59377, 2021.

[7] A. Ukil, S. Bandyoapdhyay, C. Puri, and A. Pal, "IoT healthcare analytics: The importance of anomaly detection," in 2016 IEEE 30th international conference on advanced information networking and applications (AINA), 2016: IEEE, pp. 994-997 .

[8] X.-W. Wu, Y. Cao, and R. Dankwa, "Accuracy vs Efficiency: Machine Learning Enabled Anomaly Detection on the Internet of Things," in 2022 IEEE International Conference on Internet of Things and Intelligence Systems (IoTaIS), 2022: IEEE, pp. 245-251 .

[9] A. B. Nassif, M. A. Talib, Q. Nasir, and F. M. Dakalbab, "Machine learning for anomaly detection: A systematic review," Ieee Access, vol. 9, pp. 78658-78700, 2021.

[10] P. Gogoi, D. K. Bhattacharyya, B. Borah, and J. K. Kalita, "A survey of outlier detection methods in network anomaly identification," The Computer Journal, vol. 54, no. 4, pp. 570-588, 201۱.

[11] S. Agrawal and J. Agrawal, "Survey on anomaly detection using data mining techniques," Procedia Computer Science, vol. 60, pp. 708-713, 2015.

[12] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly detection: A survey," ACM computing surveys (CSUR) ,vol. 41, no. 3, pp. 1-58, 2009.

[13] R. A. A. Habeeb, F. Nasaruddin, A. Gani, I. A. T. Hashem, E. Ahmed, and M. Imran, "Real-time big data processing for anomaly detection: A survey," International Journal of Information Management, vol. 45, pp. 289-307, 2019.

[14] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly detection for discrete sequences: A survey," IEEE transactions on knowledge and data engineering, vol. 24, no. 5, pp. 823-839, 2010.

[15] D. Mutz, F. Valeur, G. Vigna, and C. Kruegel, "Anomalous system call detection," ACM Transactions on Information and System Security (TISSEC), vol. 9, no. 1, pp. 61-93, 2006.

[16] S. Ksibi, F. Jaidi, and A. Bouhoula, "A comprehensive study of security and cyber-security risk management within e-Health systems :Synthesis, analysis and a novel quantified approach," Mobile Networks and Applications, vol. 28, no. 1, pp. 107-127, 2023.

[17] "Cybersecurity Attacks Dataset." https://www.kaggle.com/datasets/teamincribo/cyber-securityattacks/data