8th National Conference on
Modern Studies and Resech in Computer, Electrical, and Mechanical Sciences of Iran
www.ICconf.ir

هشتمین همایش ملی مطالعات و تحقیقات نوین در حوزه
علوم کامپیوتر، برق و مکانیک ایران

ارزیابی و کارایی روش های تشخیص نفوذ در اینترنت اشیاء با استفاده از یادگیری ماشینی

۱- محمدرضا کردزنگنه ۲- علیرضا هدایتی

۱- دانشجوی دکترای مهندسی نرم افزار کامپیوتر،گروه مهندسی کامپیوتر،دانشگاه آزاد اسلامی واحد تهران مرکزی

۲- استادیار گروه مهندسی کامپیوتر،دانشکده فنی و مهندسی، دانشگاه آزاد اسلامی واحد تهران مرکزی

Email:Mk66.naft@yahoo.com
Email :Hedayati@iauctb.ac.ir

چکیده:

افزایش روز افزون دستگاه های متصل به شبکه اینترنت اشیا باعث شد تا تهدیدات و خطرات احتمالی در این نوع شبکه ها بیش از هرچیز مورد توجه قرار گیرد. وجود خطرات و تهدیدات مختلف در فضای شیکه اینترنت اشیاء باعث شد راهکارهای متنوعی جهت تامین امنیت این شبکه ها مانند حفاظت از داده ها، رمز نگاری، مخابرات امن، سنسور ها و الگوریتم های رمزنگاری ارائه گردد. یکی از حوزه هایی که میتواند در مبحث تامین اینترنت اشیاء بسیار مورد توجه قرار گیرد استفاده از مفاهیم و الگوریتم های یادگیری ماشین است. بنابراین، تشخیص ناسازگاری و حملات در یک شبکه کامپیوتری و توسعه سیستم تشخیص نفوذ نقش بالقوه ای را برای امنیت سایبری انجام می‌دهد. هوش مصنوعی، به ویژه تکنیک های یادگیری ماشین، برای توسعه یک سیستم تشخیص نفوذ مورد استفاده قرار گرفته است. در این مقاله برخی از تحقیقات انجام شده در خصوص راهکارهای تامین امنیت شبکه اینترنت اشیاء با استفاده از الگوریتم ها و مفاهیم یادگیری ماشین بررسی میگردد.

کلمات کلیدی: اینترنت اشیاء ، تشخیص نفوذ، الگوریتم های یادگیری ماشین

مقدمه:

اینترنت اشیاء[1] شامل مجموعه گسترده‌ای از حسگرها، محرک‌ها و سایر دستگاه‌هایی است که در مناطق بزرگ مستقر شده و از طریق پروتکل‌هایی مانند بلوتوث، وای‌فای، و ... به هم متصل شده‌اند که برای رسیدن به اهداف مشترک همکاری می‌کنند.کاربردهای اینترنت اشیاء در زندگی روزمره انسان ها به وفور دیده میشود .از نمونه استفاده اینترنت اشیاء در سطحی ترین حالت آن میتوان به دستگاه های خانه هوشمند مانند لامپ، یخچال و گاز هوشمند، آداپتورهای هوشمند، کنتورهای هوشمند،سنسور دما، ردیاب دود و

[1] Internet of Things

هزاران مورد دیگر اشاره نمود[۱]. مقیاس عظیم شبکه های اینترنت اشیاء چالش های جدیدی را به وجود می آورد که از نمونه این چالش ها میتوان به مدیریت دستگاه ها، حجم زیادی از داده، ذخیره سازی، ارتباطات، محاسبات و امنیت و حفظ حریم خصوصی، اشاره نمود. در مقایسه با شبکه‌های کامپیوتری سنتی، اینترنت اشیاء شامل تعداد بیشتری از انواع مدل شبکه‌ها و اشیاء مرتبط با آن می‌باشد. اینترنت اشیا به دنبال ترویج مدل‌های مختلف شبکه برای تعامل بیشتر می‌باشد که این موضوع باعث ایجاد مسائل امنیتی جدیدی در اینترنت اشیا می‌شود[۲]. بسیاری از این چالش های امنیتی به دلیل جدید بودن بستر اینترنت اشیاء هنوز ناشناخته بوده و به همین دلیل به یکی از مهمترین موضوعات مورد توجه محققان این حوزه تبدیل شده است و راه کارها و چارچوب های مختلفی در این خصوص ارائه شده است.از جمله این موارد میتوان به امنیت سخت افزاری، امنیت شبکه، حفاظت از ارتباطات، استفاده از تکنیک های رمزنگاری و استفاده از راه کارهای مبتنی بر تحلیل های امنیتی اشاره کرد .یکی از راهکارهایی که در حال حاضر به شدت مورد توجه محققان حوزه امنیت اینترنت اشیا قرار گرفته است استفاده از یادگیری ماشینی[۲] در تشخیص نفوذ[۳] میباشد[۳].
راه حل های امنیتی مبتنی بر یادگیری ماشین در مقایسه با راه کارهای امنیتی سنتی اینترنت اشیا که عمدتا مبتنی بر کنترل و رمزگذاری هستند، جایگزین مناسب تری هستند .از دیدگاه تدافعی، راه کارهای سنتی نتوانسته اند امنیت شبکه های اینترنت اشیا را تامین کنند و به نظر می رسد استفاده از یک لایه اضافی از امنیت مبتنی بر یادگیری ماشین می تواند در تقویت امنیت این شبکه ها سودمند باشد. هدف این مقاله، بررسی راه کارهای ارائه شده در تشخیص نفوذ در اینترنت اشیا بر مبنای استفاده از مفاهیم و الگوریتم های یادگیری ماشینی است[۴].

سیستم تشخیص نفوذ در اینترنت اشیاء

تشخیص نفوذ ، انجام اقداماتی جهت تشخیص نفوذگران و مهاجمان به سیستم های اطلاعاتی است.سیستم تشخبص نفوذ شامل حسگرها، موتورتحلیل، و سیستم گزارش دهی است. وظیفه این حسگرها جمع آوری داده های شبکه یا میزبان از قبیل آمارهای ترافیکی ،سرآیند بسته ها،درخواست های سرویس و فراخوان های سیستم عامل است که طبق معماری شبکه آن را در مکان های مختلف قرار می دهد.حسگرها داده های جمع آوری شده را به موتورهای تحلیل ارسال میکنند، که مسئولیت بررسی داده های جمع آوری شده و تشخیص نفوذ های در حال انجام را با رویکردهای مختلف، مبتنی بر امضا، مبتنی بر ناهنجاری، مبتنی بر مشخصه، و مبتنی بر روش ترکیبی دارد. وقتی موتور تحلیل، نفوذی را تشخیص می دهد، سیستم گزارش دهی را با اطلاعات نفوذ شامل شناسایی نفوذ کننده، محل نفوذ، زمان نفوذ، و نوع نفوذ مجهز می کند و این سیستم هشداری را برای مدیر شبکه تولید میکند[۵].

امروزه برای برقرای امنیت و ارتباطات و تبادل اطلاعات، اقدامات متنوعی از قبیل رمز نگاری اطلاعات، طراحی پروتکل های امن، به کارگیری دیواره های آتش، و سیستم های ردیابی و جلوگیری از نفوذ از طریق سیستم های تشخیص نفوذ انجام شده است. از انجا که در بسیاری از حوادث ایجاد شده در شبکه ، مهاجم یک انسان یا یک برنامه هوشمند است، نیاز به یک روشی است که به تناسب

[۲] machine learning
[۳] Intrusion detection

اقدامات پیشگیرانه و متقابل مدافعین را تغییر دهد.به همین دلیل در سال های اخیر روش های یادگیری ماشینی در حوزه امنیت شبکه آغاز شده است[۶].

راهکارهای یادگیری ماشین در تشخیص نفوذ

تهدیدات و ریسک های موجود در شبکه های اینترنت اشیاء باعث ایجاد انگیزه جهت استفاده از تکنیک های شناسایی و مسدود کردن حملات ترافیک در این شبکه ها با استفاده از یادگیری ماشین گردید. راه حل های امنیتی مبتنی بر یادگیری ماشین گزینه های قابل قبولی برای جایگزینی با روش های تامین امنیت سنتی که تمرکز آنها بر کنترل دسترسی و کدگذاری بوده است، میباشد. هرچند از دیدگاه مقابله با تهدیدات، این روش ها محکوم به شکست بوده و وجود یک لایه اضافی از امنیت مبتنی بر یادگیری ماشین می تواند در تقویت امنیت سودمند باشد .روش های یادگیری ماشین در یک دیدگاه کلی به سه دسته اصلی تقسیم شده است که عبارتند از :یادگیری نظارت شده، نظارت نشده و تقویتی، هرچند، دسته بندی های دیگری نیز وجود دارد. به عنوان مثال، با توجه به میزان در دسترس بودن داده های یک شبکه، این روش ها میتوانند به دو دسته مبتنی بر شبکه و مبتنی بر میزبان تقسیم شوند. محققان به ارائه دسته بندی ها و چگونگی ارتباط الگوریتم ها و اثربخشی آنها در یادگیری ماشین اشاره نموده است .این دسته بندی ها در جدول ۱ ارائه شده است[۷].

جدول ۱ دسته بندی تکنیک های یادگیری ماشین[۷]

تکنیکهای یادگیری ماشین	روشهای یادگیری	الگوریتم های مرتبط	محدویتهای محاسبتی	نرخ از دست دادن دیتا
مبتنی بر شبکه	یادگیری نظارت شده	CNN و ADA	کم	زیاد
	نظارت نشده	DBSCAN	کم	زیاد
	تقویتی	DQN و SARSA	متوسط	زیاد
مبتنی بر میزبان	یادگیری نظارت شده	k-NN و SVM	زیاد	کم
	نظارت نشده	k-Means و GGMs	زیاد	کم
	تقویتی	Q-Learning	زیاد	متوسط

پیشینه پژوهش:

در سال های اخیر مقالات و روش های مختلف مبتنی بر یادگیری ماشین در حوزه تشخیص نفوذ در اینترنت اشیاء به منظور تحلیل و بهینه سازی عملکرد و کارایی سیستم های تشخیص نفوذ در فناوری های مرتبط با اینترنت اشیاء منتشر شد که می توان به موارد زیر اشاره کرد.

در مطالعه ای که نسا و همکارانش انجام داده اند، یک مکانیزم تشخیص برای داده های پرت و ناسالم در شبکه های اینترنت اشیاء ارائه نموده اند .آنها از روش غیر پارامتری استفاده کرده اند که به دلیل اینکه این روش ها نیازی به فضای ذخیره سازی بزرگی جهت نگهداری داده های ورودی ندارند، برای داده های شبکه اینترنت اشیاء مناسب هستند .همچنین در این مطالعه از یادگیری نظارت شده مبتنی بر توالی استفاده نموده اند که برای تشخیص داده های پرت مناسب هستند .نتایج این تحقیق نشان داد که نرخ تشخیص در دیتابیس های مختلف ٪ ۹۹،۶۵ و ٪ ۹۸،۵۳ بوده است[۸].

در مقاله دامینگ و همکاران نکات برجسته استخراج اینترنت اشیاء و الگوریتم های تشخیص وقفه برای شهر هوشمند مبتنی بر حرکت در مدل یادگیری پیشنهاد شده است که به مدل عمیق نوآوری مکان وقفه با یادگیری می پیوندد .با توجه به محاسبه در دسترس، یک مدل یادگیری که نشان دهنده جابجایی نقشه و ویژگی های داده کاوی است در این مقاله معرفی شده است .در بخش آزمایشی، ۹۹ KDD CUP به عنوان مجموعه ای از اطلاعات آزمایش انتخاب شده و ۱۰ درصد از این اطلاعات به عنوان اطلاعات آماده سازی استفاده شدند به طور همزمان، محاسبه پیشنهادی و الگوریتم های موجود مقایسه شدند .نتایج نشان داد که محاسبه پیشنهادی باعث برجسته تر شدن برخی حافظه های کوتاه تر و بهره وری مکان میشود در این پژوهش از روش SVM[۴]استفاده گردید[۹].

در مقاله آراچیگه و همکارانش چارچوبی به نام PriModChain معرفی گردید که هدف آن حفظ محرمانگی و قابلیت اعتماد در داده های اینترنت اشیاء صنعتی با استفاده از الگوریتم های ترکیبی یادگیری ماشین، بلاکچین و ... است .امکان سنجی این چارچوب با معیارهای پنج گانه محرمانگی، امنیت، قابلیت اطمینان، ایمنی و بازیابی توسط شبیه سازی که با استفاده از پایتون و برنامه نویسی سوکت بر روی یک کامپیوتر با کاربری عمومی، ارزیابی شد .همچنین برای تست این چارچوب از الگوریتم شبکه عصبی استفاده شد . این چارچوب نتایج بسیار خوبی را بر مبنای پنج رکن قابل اعتماد تولید نموده و ثابت کرد که یک راه حل مناسب برای قابلیت اعتماد و حفظ محرمانگی در سیستم های اینترنت اشیاء صنعتی است[۱۰].

در مقاله جانیاد ارشاد و همکارانش یکی از تجهیزات تشخیص نفوذ محدود مربوط به ساختار انرژی پیشنهاد شده است که اساس زیست بوم اینترنت اشیا را تشکیل می دهد .با توجه به ماهیت موقت این سیستم ها و همچنین تهدیدات نوظهور و پیچیده مانند باتنت(ربات شبکه)، آن ها احتمال ترکیب میزبان(دستگاه های اینترنت اشیا) و ابزارهای پیشرفته را برای تشخیص موثر نفوذ و در عین حال به حداقل رساندن هزینه های مصرف انرژی و ارتباطات ارزیابی می کنند .آن ها چارچوب پیشنهادی را با سیستم عامل اجرا می کنند و ارزیابی دقیقی از پتانسیل بازده ارزیابی متقابل انجام می دهند .نتایج ارزیابی نشان می دهد که چارچوب پیشنهادی می تواند میزان توان و ارتباطات را کاهش دهد، در حالی که سیستم های تشخیص نفوذ مشارکتی اینترنت اشیا را ممکن می سازد. [۱۱].

[۴] Support vector machines

کلاتون اپدا کاستا و همکارانش روش جدیدی را پیشنهاد کردند که بر اساس مقالات پیشرفته و دقیق در مورد روش های یادگیری ماشین مبتنی بر اینترنت و تشخیص نفوذ برای امنیت شبکه رایانه ای است. بنابراین، این پروژه بر جستجوهای اخیر و عمیق برای مقالات مرتبط در مورد روش‌های مختلف هوشمند و ساختارهای تشخیص نفوذ اعمال شده در شبکه های رایانه ای، با تأکید بر اینترنت اشیا و یادگیری ماشین متمرکز شده است. در این پژوهش از روش SVM با CSOACN ها استفاده گردید که دارای دقت حدود ۹۸ درصد است [۱۱].در جدول زیر، اطلاعات دقیقی در مورد فناوری ها و کارایی آن ها ارائه نموده ایم.

جدول ۲ ارزیابی و کارایی روش های تشخیص نفوذ در اینترنت اشیاء

شماره	نام نویسنده	روش	دقت	هدف
۱	نسا و همکاران	روش غیر پارامتری و یادگیری نظارت شده مبتنی بر توالی	٪ ۹۹.۶۵و٪ ۹۸.۵۳	مکانیزمی جهت شخیص برای داده های پرت و ناسالم در شبکه
۲	دامینگ و همکاران	SVM	دسته بندی داده و زمان الگوریتم می تواند به صورت موثری کاهش یابد	یک سیستم آشکار سازی نفوذ، وجود مشکل در شبکه را تشخیص می دهد
۳	آراچیگه و همکارانش	چارچوبی به نامPriModChain	راه حل مناسب برای قابلیت اعتماد و حفظ محرمانگی در سیستم های اینترنت اشیا صنعتی	حفظ محرمانگی و قابلیت اعتماد در داده های اینترنت اشیاء صنعتی
٤	جانیاد ارشاد و همکارانش	K-NNو میانگینK	و انرژی نمودن حداقل ارتباطات کلی	برای بررسی چالش ها در آشکارسازی نفوذ برای اینترنت اشیاء
٥	کلاتون اپدا کاستا و همکارانش	روش SVM با CSOACN	مقدار دقت حدود۹۸ درصد است	CCNعملکردی عالی در تجسم و ارتباطات دارد

نتیجه گیری

امروزه استفاده از اینترنت اشیاء بسیار گسترده شده و همین امر منجر به ایجاد مخاطرات و تهدیدهای امنیتی بسیار گشته است . بسیاری از این دستگاه ها در شبکه اینترنت اشیا ءاساساً ناامن هستند و شبکه را در معرض انواع حملات قرار می دهند .از همین رو به بررسی راه کارهای بهبود تشخیص نفوذ در شبکه های اینترنت اشیاء روی آورده و راه کارهای متنوعی ارائه شد .در بین راه حل های موجود استفاده از مفاهیم یادگیری ماشین بیش از سایر روش ها مورد استقبال قرار گرفت زیرا این راه کارها جایگزین مناسبی برای روش های سنتی در حوزه تشخیص نفوذ هستند. نتایج نشان داد که استفاده از الگوریتم های یادگیری ماشین نظارت شده، یک راهکار موثر با تفکیک بین دسته آسیب دیده و نیرومند با دقت زیاد است. در این مقاله به بررسی برخی از مطالعات انجام شده

در حوزه تشخیص نفوذ در اینترنت اشیاء با استفاده از روش های یادگیری ماشین ازجمله روش غیر پارامتری و یادگیری نظارت شده مبتنی بر توالی، SVM ، چارچوب PriModChain، و روش SVM با CSOACN پرداخته شد که نتایج قابل توجهی را در بر داشته اند.

منابع:

1-Towards Machine Learning Based Intrusion Detection in IoT Networks, Institute of Information Technology, Jahangirnagar University, Dhaka, Bangladesh, Received: 08 March 2021; Accepted: 09 April 2021
2-T. Perković, S. Damjanović, P. Šolić, L. Patrono, and J. J. Rodrigues, "Meeting Challenges in IOT: Sensing, Energy Efficiency, and the Implementation," in Fourth International Congress on Information and Communication Technology, 2020, pp. 419-430: Springer.
3- K. Tabassum, A. Ibrahim, and S. A. El Rahman, "Security issues and challenges in IOT," in 2019 International Conference on Computer and Information Sciences (ICCIS), 2019
4- F. Hussain, R. Hussain, S. A. Hassan, and E. Hossain, "Machine learning in IOT security: current solutions and future challenges," IEEE Communications Surveys & Tutorials, 2020.
5- S. Zeadally and M. Tsikerdekis, "Securing Internet of Things (IOT) with machine learning," International Journal of Communication Systems, vol. 33, no. 1, p. e4169, 2020.
6- L. E. Kane, J. J. Chen, R. Thomas, V. Liu, and M. Mckague, "Security and Performance in IOT: A Balancing Act," IEEE Access, vol. 8 , pp. 121969-121986, 2020.
7- N. M. Radwan, "A Study: The Future of the Internet of Things and its Home Applications," International Journal of Computer Science and Information Security (IJCSIS), vol. 18, no. 1, 2020.
8-N. Nesa, T. Ghosh, and I. Banerjee, "Non-parametric sequence-based learning approach for outlier detection in IOT," Future Generation Computer Systems, vol. 82, pp. 412-421, 2018.
9- Daming Li, Minhang Lee LianbingDeng, Haoxiang Wang, IoT data feature extraction and intrusion detection system for smart cities based on deep migration learning, Int J Inf Manage 49 (2019) 533–545. 10-P. C. M. Arachchige, P. Bertok, I. Khalil, D. Liu, S. Camtepe, and M. Atiquzzaman, "A trustworthy privacy preserving framework for machine learning in industrial IOT systems," IEEE Transactions on Industrial Informatics, vol. 16, no . 9 , pp. 6092-6102, 2020.
10-Junaid Arshad, Muhammad Ajmal Azad, Muhammad Mahmoud Abdeltaif, Khaled Salah, An intrusion detection framework for energy-constrained IoT devices, Mech. Syst. Signal. Process. 136 (2020), 106436.
11- Georgios Tertytchny, Nicolas Nicolaou, Maria K. Michael, Classifying network abnormalities into faults and attacks in IoT-based cyber physical systems using machine learning, Microprocess. Microsyst. 77 (2020), 103121. ISSN 0141-9331.