باسمه تعالی

پوریا دادخواه - 401201381

شرح مختصر موضوع پروژه: "تحلیل سامانه‌های تشخیص نفوذ مبتنی بر یادگیری عمیق در شبکه‌های اینترنت اشیاء"

حملات سایبری از درون شبکه یا سیستم هدف و یا از خارج سیستم و از دستگاه‌های خارجی، ازجمله تهدیدات مهم موجود هستند. در سالیان گذشته ابزارهای گوناگونی از دیوارهای آتش تا سیستم‌های تشخیص نفوذ و پیشگیری نفوذ و هانی‌پات‌ها برای مقابله با این حملات معرفی و استفاده شده‌اند. ضعف و نقص سایر ابزار باعث شده است که وجود سیستم‌های تشخیص نفوذ در اکثر کاربردها حیاتی باشد. دیوارهای آتش و سایر سیستم‌های مشابه، دو نقطه ضعف اساسی دارند. اول آن‌که به‌دلیل نحوه تحلیل داده‌های ورودی، توانایی تشخیص حملات و نفوذ با منشأ شبکه داخلی را ندارند، دوم این‌که به‌دلیل قاعده‌محور بودن این روش‌ها و طراحی بسته‌ی خود، حملات نوظهور را تشخیص نخواهند داد. از طرف دیگر، ابزارهایی مانند هانی‌پات‌ها با این‌که توانایی قابل قبولی برای تشخیص حملات جدید خارجی و داخلی را دارند، اولا به‌تنهایی برآورده‌کننده امنیت سیستم اصلی نیستند و تنها یک ابزار فرعی در کنار آن هستند که به بهبود آن کمک می‌کنند، ثانیا در همه سیستم‌ها و شبکه‌ها خصوصا IoT قابلیت پیاده‌سازی ندارند ،چرا که نیازمند منابع پردازشی و فیزیکی بوده که بسته به کاربرد لزوما راه‌حل به صرفه‌ای محسوب نخواهند شد. بنابراین وجود سیستم‌های تشخیص نفوذ در صنعت با قابلیت‌هایی نظیر تحلیل و نظارت پیوسته شبکه داخلی، یادگیری از داده‌های قبلی و موجود و نیز عملکرد مناسب در برابر حملات با منشأ خارجی می‌تواند در کنار سایر ابزارهای اشاره‌شده امنیت قابل توجهی را فراهم سازد. سیستم‌های تشخیص نفوذ بر اساس وظیفه تعریف شده و عملکردشان در معماری شبکه به دو دسته کلی میزبان-محور و مبتنی بر شبکه تقسیم می شوند. در سیستم‌های میزبان-محور با دسترسی و بررسی داده‌های ورودی به یک سیستم مشخص از شبکه، سالم بودن ترافیک تشخیص داده می شوند و در سیستم‌های مبتنی بر شبکه بسته به نوع کاربرد، ترافیک‌های موجود در کل شبکه بررسی می‌شود و هریک را به دسته‌های سالم و یا خرابکار تخصیص می‌دهد. به‌طور کلی یک سیستم تشخیص نفوذ بنا به نوع خود، منابع مختلف داده مانند ترافیک شبکه، گزارش‌های امنیتی، ویژگی‌های شیوه‌نامه، داده‌های میزبان، اندازه‌گیری حسگرها، داده‌های حسابرسی و اطلاعات سامانه را تحلیل می‌کند تا رفتارهای غیرعادی، فعالیت مخرب و نقض سیاست‌های تعریف شده در سامانه را تشخیص دهد. علاوه بر این شواهدی را فراهم می‌کند و به اطلاع راهبر می‌رساند تا واکنش‌های مناسبی را نسبت به حملات سایبری اعمال کند. در این راستا بررسی سازوکارها و راهبردهای مختلف در طراحی یک سیستم تشخیص نفوذ ازجمله روش‌های برپایه یادگیری ماشین به همراه روش‌های آماری بسیار کمک کننده و نیازمند پژوهش کافی است.

سیستم‌های تشخیص نفوذ مبتنی بر شبکه IoT که محور اصلی پژوهش آتی خواهد بود می‌توانند با قرارگیری در مسیر عبور داده‌های شبکه، از طریق اتصال به سوییچ‌ها و جمع‌آوری کل داده‌های ورودی، بر محتوای بسته‌های شبکه نظارت و درصورت لزوم آن‌ها را ضبط کنند. الگوریتم‌های مورد بررسی در این پژوهش مبتنی بر یادگیری عمیق هستند که دارای مزایای ارزشمندی نظیر داشتن دقت تشخیص بسیار بالا در عین داشتن نرخ هشدارهای مثبت اشتباه[1] به مراتب پایین‌تر نسبت به سایر الگوریتم‌های یادگیری ماشین خواهند بود. علاوه بر آن قابلیت تشخیص حملات ناشناخته را خواهند داشت که مزیت آن‌ها را نسبت به طرح‌های قدیمی‌تر مانند سیستم‌های برپایه امضا و قانون نشان می‌دهد . در این پروژه قصد داریم با بررسی تئوری این الگوریتم‌ها و پیاده‌سازی نمونه موفقی از آن‌ها به تحلیل عملکرد و چالش‌های این نوع از IDSها بپردازیم.

[1] Youcef Djenouri,Asma Belhadi, Gautam Srivastava , Jerry Chun-Wei Lin" Emergent Deep Learning for Anomaly Detection in Internet of Everything" IEEE INTERNET OF THINGS JOURNAL, VOL. 10, NO. 4, 15 FEBRUARY 2023

[2] Tahmina Zebin,Shahadate Rezvy , Yuan Luo." An Explainable AI-based Intrusion Detection System for DNS over HTTPS (DoH) Attacks"IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 0, NO. 0, DECEMBER 2021

[3] Yixuan Wu , Laisen Nie, Shupeng Wang, Zhaolong Ning and Shengtao Li." Intelligent Intrusion Detection for Internet of Things Security: A Deep Convolutional Generative Adversarial Network-Enabled Approach" IEEE INTERNET OF THINGS JOURNAL, VOL. 10, NO. 4, 15 FEBRUARY 2023

[1] False Positive Rate