به نام خدا

دانشگاه صنعتی امیرکبیر

تمرین اول روش پژوهش و ارائه

انتخاب موضوع تحقیق

تشخیص نفوذ شبکه‌های کامپیوتری مبتنی بر یادگیری‌ماشین

استاد درس: دکتر رضا صفابخش

دانشجو: بهار کاویانی

شماره دانشجویی: ۹۷۳۱۰۵۱

نیم‌سال دوم ۰۰-۹۹

سوال اول:

با بررسی موضوعی که برای کار تحقیقاتی خود انتخاب کرده‌اید، یک متن توضیحی در حدود نصف صفحه نوشته و مراجع مربوطه را لیست نمایید.

امروزه امنیت شبکه یکی از مسایل پیچیده و بسیار مهم حوزه‌ی شبکه‌های کامپیوتری است. با گسترش روز افزون این دانش و تکنولوژی، حملات سایبری و نفوذ به شبکه‌های کامپیوتری نیز گسترده‌تر شده‌است. در چنین شرایطی برای ایجاد امنیت کامل، تنها راه‌کارهای مقابله با نفوذ همانند استفاده از فایروال‌ها نمی‌توانند راه‌گشای ما در این مسیر باشند و مهندسان شبکه به روش‌هایی برای شناسایی و تشخیص نفوذ به سیستم‌ها و شبکه‌های کامپیوترها نیاز دارند تا بتوانند راه‌حل‌ها و الگوریتم‌های جدیدی را به وجود بیاورند. در حقیقت سیستم‌ها می‌توانند با کمک تشخیص نفوذ[1] رفتارهای خراب‌کار را بشناسند و از خود در برابر این حملات محافظت کنند.

الگوریتم‌های یادگیری ماشین می‌توانند برای شناسایی و یا جلوگیری از حملات شبکه، دقت بهتر و سرعت تشخیص بیش‌تری را برای ما به ارمغان آورند. از طرفی یکی دیگر از مزایای استفاده از یادگیری ماشین این است که دیگر برای تشخیص نفوذ شبکه به تجربه و دانش کارشناسان و متخصصین نیازی نخواهیم داشت.

منابع:

[۱] کاظمی‌تبار، سید جواد و طاهری امیری، ریحانه و خردمندیان، قربان "ارائه روشی جدید جهت بهبود تشخیص نفوذ با استفاده از ترکیب الگوریتم جنگل تصادفی و الگوریتم ژنتیک" نشریه علوم و پدافند نوین، پاییز ۱۳۹۸

[۲] ویسی، هادی و موسوی، سیدهادی و خوانساری، محمد "تشخیص حملات شبکه‌های کامپیوتری با یادگیری ماشین و تحلیل داده‌های جریان ترافیک" نشریه علمی فناوی اطلاعات و ارتباطات انتظامی، دانشگاه تهران، شماره ۱، بهار ۱۳۹۹

[3] C.-S. Lee, Y.Su, Y. Lin "Machine Learning Based Network Intrusion Detection" 2nd IEEE International Conference on Computational Intelligence and Applications, 2017

[4] R. Abdulhammed, H. Musafer, A. Alessa, M. Faezipour, A. Abuzneid "Features Dimensionality Reduction Approaches for Machine Learning Based Network Intrusion Detection" University of Bridgeport, March 2019

[5] H. Liu, B. Lang "Machine Learning and Deep Learning Methods for Intrusion Detection Systems: A Survey" Beihang University, October 2019

[6] M. Sarhan, S. Layeghy, N. Moustafa, M. Portmann "NetFlow Datasets for Machine Learning-based Network Intrusion Detection Systems"

[1] Intrusion Detection System (IDS)

[۷] نجار، مرضیه و معطر، محمدحسین "تشخیص نفوذ شبکه با استفاده از رویکرد ترکیبی مدل مخفی مارکوف و یادگیری ماشین مفرط"مجله مهندسی برق دانشگاه تبریز، جلد ۴۸ ، شماره ۴، زمستان ۱۳۹۷

[۸] علی‌پور، حسن و نیری‌فرد، طاهره "بررسی مشکلات و جدیدترین رویکردهای تست نفوذ با هدف بهبود روش‌های کنونی" دانشگاه علمی کاربردی جهاد دانشگاهی

[9] Y. Otoum, A. Nayak "AS-IDS: Anomaly and Signature Based IDS for the Internet of Things" February 2021

سوال دوم:

این پروژه چه اهدافی را دنبال می‌کند؟ (آرمانی، کلی، ویژه و یا کاربردی)

هدف آرمانی پژوهش:

دست‌یابی به الگوریتمی مبتنی بر یادگیری ماشین برای تشخیص نفوذ به شبکه‌های کامپیوتری که نقطه ضعفی در انجام وظیفه‌ی خود نداشته باشد و در مقایسه با سایر برنامه‌ها، الگوریتمی ساده و در عین حال سریع و دقیق داشته باشد.

هدف کلی پژوهش:

بررسی و مقایسه‌ی الگوریتم‌های مهم و مبتنی بر یادگیری ماشین در زمینه‌ی تشخیص نفوذ به شبکه‌های کامپیوتری

اهداف ویژه‌ی پژوهش:

۱. تعیین میزان تاثیر هر الگوریتم بررسی شده در سرعت تشخیص نفوذ

۲. تعیین میزان حافظه‌ی مورد نیاز هر الگوریتم بررسی شده برای تشخیص نفوذ

۳. تعیین نقاط ضعف هر الگوریتم بررسی شده در تشخیص نفوذ

اهداف کاربردی پژوهش:

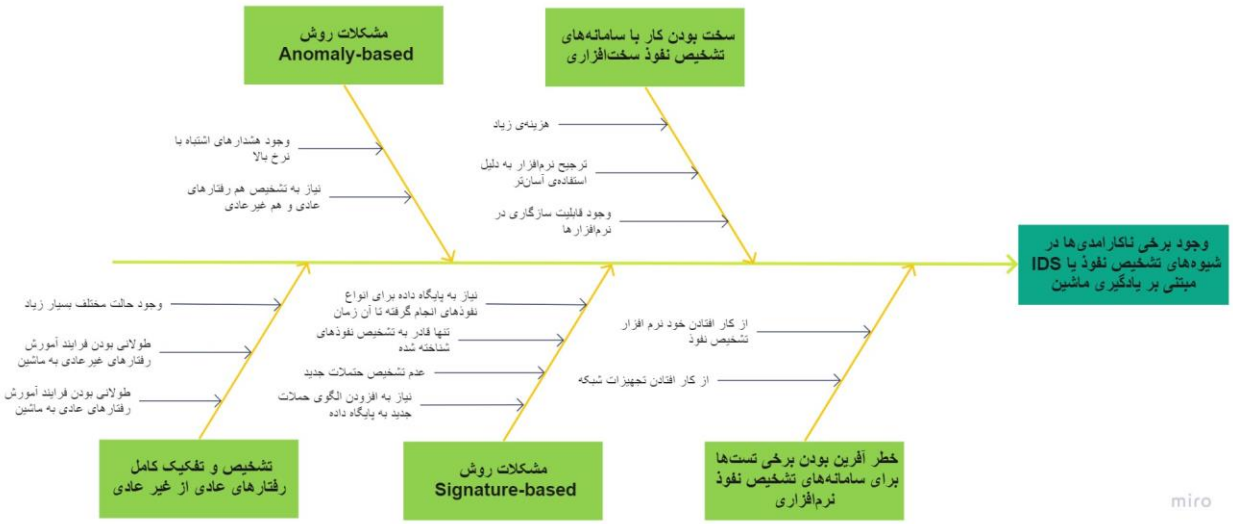
۱. تعیین مناسب‌ترین الگوریتم از نظر سرعت در تشخیص نفوذ به شبکه‌های کامپیوتری

۲. تعیین مناسب‌ترین الگوریتم از نظر دقت در تشخیص نفوذ به شبکه‌های کامپیوتری

۳. تعیین مناسب‌ترین الگوریتم از نظر حافظه‌ی مورد نیاز در تشخیص نفوذ به شبکه‌های کامپیوتری

سوال سوم:

تحقیق موردنظر قصد برطرف کردن چه مشکلی را دارد؟ برای این مشکل یک دیاگرام استخوان ماهی رسم کنید.



سوال چهارم:

برای تعریف موضوع تحقیقاتی خود، بررسی جزییات را در یک نقشه‌ی ذهن نمایش دهید.