چهارمین کنفرانس بین المللی
مطالعات نوین در علوم کامپیوتر و فناوری اطلاعات
4th International Conference
On New studies Of Computer And IT
FEBRUARY 24,2018
مشهد
۰۵ اسفند ماه ۱۳۹۶

ارائه‌ی سیستم تشخیص نفوذ براساس یادگیری جمعی و تلفیق داده

مریم یوسف نژاد[۱]، جواد حمید زاده[۲]

۱-دانشجوی کارشناسی ارشد مهندسی کامپیوتر و فناوری اطلاعات، دانشگاه صنعتی سجاد، مشهد

۲-عضو هیئت علمی، دانشکده مهندسی کامپیوتر و فناوری اطلاعات، دانشگاه صنعتی سجاد، مشهد

چکیده

سیستم تشخیص نفوذ یک سیستم امنیتی می‌باشد، که خرابکاری‌ها و نفوذهای روی شبکه را شناسایی می کند و حملات و سوء استفادهای که از شبکه و سیستم می‌شود را به مسئولان اطلاع می‌دهد. روش‌های مختلف طبقه‌بندی تکی همچون الگوریتم ژنتیک، فازی، درخت تصمیم، شبکه عصبی، ماشین بردار پشتیبان در سیستم تشخیص نفوذ مورد استفاده قرار گرفته‌اند، این روش‌ها هر کدام دارای مزایا و معایبی می‌باشند اما نسبت به بعضی روش‌های ترکیبی دقت کمتری دارند. در دهه اخیر تشخیص مبتنی بر ناهنجاری و بسیاری از مشکلات طبقه‌بندی از ایده ترکیب طبقه‌بند استفاده می کنند در این مقاله برای بهبود عملکرد، دقت و کاهش هشدار اشتباه در سیستم تشخیص و نفوذ، روش یادگیری جمعی پیشنهاد شده است. طبقه‌بند KNN برای تشخیص ناهنجاری و مشکلات چند کلاسه می‌باشد و برای ترکیب خروجی چندگانه KNN از روش تلفیق داده دمپستر شافر که خروجی آن به صورت چند کلاسه امتیاز دار و امکان بازیابی صریح عدم قطعیت را دارد بکار گرفته شده است. آزمایشات بر روی مجموعه داده NSL-KDD انجام شده است نتایج آزمایشات نشان برتری دقت روش پیشنهادی نسبت به طبقه‌بندهای بکار رفته در روش پیشنهادی است. همچنین روش پیشنهادی دقت بیشتری در بعضی حملات، نسبت به سایر روش‌های ترکیب طبقه‌بند همچون رأی اکثریت و روش ترکیب الگوریتم SVM و KNN با استفاده از الگوریتم رأی اکثریت در این زمینه را دارد.

واژگان کلیدی: تشخص و نفوذ، نزدیکترین همسایگی، یادگیری جمعی، تئوری دمپسترشافر، تلفیق داده.