6TH INTERNATIONAL CONFERENCE ON APPLIED RESEARCH IN COMPUTER, ELECTRICAL AND INFORMATION TECHNOLOGY
March 6, 2022
Tbilisi - Georgia
CINVU
Kosar University
Avicenna International Community College LLC

مروری برروی‌کردهای انتخاب ویژگی و طبقه بندی در سیستم های تشخیص نفوذ

تکتم پازش [۱] ، حسن شاکری [۱]، عابدحسینی[۲]، محمدعلی شیخ الطایفه[۳]

۱- گروه مهندسی کامپیوتر،واحد مشهد،دانشگاه آزاد اسلامی،مشهد،ایران.

۲-گروه مهندسی برق،واحد مشهد،دانشگاه آزاد اسلامی،مشهد،ایران.

۳- گروه مهندسی عمران،واحد مشهد،دانشگاه فردوسی،مشهد،ایران.

چکیده

سیستم تشخیص نفوذ دستگاه یا برنامه نرم افزاری است که شبکه یا سیستم ها را از نظر فعالیت های مخرب یا نقض خط مشی ها کنترل می‌کند. یکی از چالش های مهم در این زمینه، تشخیص درست حالت نرمال و حمله در سیستم می‌باشد. داده ها به طور کلی به دو دسته حمله و نرمال تقسیم می‌شوند. پژوهش های بسیاری در زمینه سیستم های تشخیص نفوذ مبتنی بر روش های یادگیری ماشین و یادگیری عمیق صورت گرفته است. روش‌های صورت گرفته با وجود داشتن مزایایی که به همراه داشته‌اند به دلایلی از جمله پیچیدگی محاسباتی، زمان اجرای طولانی و دیگر موارد قادر به رسیدن به دقت مطلوب در سیستم‌های تشخیص نفوذ نبوده‌اند. همچنین به دلیل تنوع وپیچیدگی حملات جدید افزایش دقت تشخیص همچنان به عنوان یک چالش باقی مانده است. دراین تحقیق به بررسی تکنیک‌های یادگیری ماشین و یادگیری عمیق در زمینه افزایش دقت سیستم‌های تشخیص نفوذ پرداخته ایم. نشان داده‌ایم که ترکیب این دو تکنیک در کنار روش‌های پیش پردازش و انتخاب ویژگی می‌توان دقت را در سیستم‌های تشخیص نفوذ افزایش داد. همچنین بیشترین مجموعه داده مورد استفاده در سیستم‌های تشخیص نفوذ NSL-KDD و ابزار پیاده سازی پایتون می‌باشد.

کلمات کلیدی: سیستم تشخیص نفوذ،تکنیک‌های یادگیری ماشین، تکنیک‌های یادگیری عمیق، پایتون، پایگاه داده NSL-KDD