

## عنوان مقاله:

هوش مصنوعی و امنیت شبکه: چالش ها و رویکردها

## محل انتشار:

دومین کنفرانس دانشجویان مهندسی کامپیوتر و فناوری اطلاعات و ارتباطات (سال: 1402)

تعداد صفحات اصل مقاله: 11

## نویسندگان:

باقر آبیاری - کارشناسی ارشد مهندسی فناوری اطلاعات، موسسه آموزش عالی غیرانتفاعی الکترونیکی فاران (مهردانش). تهران، ایران

علی سلیمانی - استادیار گروه علوم کامپیوتر. دانشگاه آزاد اسلامی. واحد ملارد. ملارد. ایران

## خلاصه مقاله:

حمله به شبکه های رایانه ای هر روز پیچیده تر می شود. تعداد بی شماری از مهاجمان حرفه ای به دنبال کسب سودهای بالا، منابع و مهارت های خود را در جرایم سایبری افزایش می دهند تا بتوانند به طور موثرتری ایجاد خسارت کنند. یکی از چالش های اصلی امنیت شبکه این است که حملات اغلب ظاهر و بردار خود را تغییر می دهند. در صورت وقوع حمله جدید به یک شبکه، تشخیص و شناسایی این رفتارها برای سیستم های سنتی امکان پذیر نیست. زیرا هیچ قانون ثابت یا الگویی برای مطابقت وجود ندارد. از این رو، راهکارهای سنتی امنیت شبکه نیازمند رویکردی هوشمندانه تر برای تشخیص تهدیدها هستند. تکنیک های یادگیری ماشین و یادگیری عمیق به عنوان زیرمجموعه هوش مصنوعی در دهه گذشته محبوبیت بسیار زیادی در زمینه امنیت شبکه به دست آورده اند. هوش مصنوعی می تواند به سازمان ها در شناسایی روند و الگوهای حوادث امنیتی کمک کند و آن ها را قادر می سازد تا کنترل های امنیتی موثرتری را اجرا کنند. با توجه به نقش هوش مصنوعی در امنیت شبکه. در این پژوهش اهمیت تکامل تکنیک های امنیت سایبری بر پایه هوش مصنوعی و ارزیابی همه جانبه چالش ها و رویکردهای پیش رو مدنظر قرار گرفته است.

## کلمات کلیدی:

امنیت شبکه، هوش مصنوعی، یادگیری ماشین، یادگیری عمیق

## لینک ثابت مقاله در پایگاه سیویلیکا:

<https://civilica.com/doc/1796767>

