

عنوان مقاله:

تشخیص حملات منع سرویس توزیع شده در دستگاه های اینترنت اشیا با استفاده از شبکه عصبی پیچشی

محل انتشار:

دومین کنفرانس ملی کسب و کار نوین در مهندسی برق و کامپیوتر (سال: 1403)

تعداد صفحات اصل مقاله: 8

نویسندگان:

امید طاهری - کارشناسی ارشد گروه مهندسی کامپیوتر، دانشگاه صنعتی همدان، همدان

فاطمه امیری - استادیار گروه مهندسی کامپیوتر، دانشگاه صنعتی همدان، همدان

جعفر فرمانی - مربی، دانشگاه فنی حرفه ای، همدان

خلاصه مقاله:

در این مقاله، به بررسی استفاده از مدل های شبکه های عصبی کانولوشنی برای تشخیص حملات در ترافیک شبکه می پردازیم. هدف اصلی این تحقیق، معرفی راه حل های مناسب برای تشخیص حملات به شبکه ها و دستگاه های مربوط به اینترنت اشیا است. برای ارزیابی عملکرد مدل پیشنهادی، از مجموعه داده UNSW-NB15 استفاده شده است. در ابتدا، داده ها پیش پردازش و ویژگی های مهم استخراج میشوند. سپس، مدل شبکه ی عصبی کانولوشنی بر روی این داده ها آموزش داده میشود. نتایج آزمایشها نشان میدهد که مدل شبکه عصبی پیچشی با دقت بالای ۹۷٪ قادر به تشخیص حملات است و عملکرد بسیار خوبی دارد. این نتایج نشان می دهد که استفاده از مدل های یادگیری عمیق، به ویژه شبکه های عصبی کانولوشنی، میتواند بهبود قابل توجهی در امنیت شبکه های اینترنت اشیا ایجاد کند. به طور خلاصه، استفاده از مدل های شبکه های عصبی کانولوشنی به عنوان روشی قوی برای تشخیص حملات در ترافیک شبکه مورد بررسی قرار گرفته است. این روش، امکان بهبود امنیت شبکه های اینترنت اشیا را فراهم میکند و میتواند به عنوان یک راهکار موثر در حوزه امنیت شبکه مورد استفاده قرار گیرد.

کلمات کلیدی:

تشخیص حملات، مدل CNN، یادگیری عمیق، ترافیک شبکه، اینترنت اشیا

لینک ثابت مقاله در پایگاه سیویلیکا:

<https://civilica.com/doc/2032462>

