عنوان مقاله:
تشخیص حملات سایبری در سیستمهای کنترل صنعتی با یادگیری عمیق ویژگیها و ماشین یادگیری شدید (ELM)

محل انتشار:
سومین کنفرانس ملی فناوری در مهندسی برق و کامپیوتر (سال: 1397)

تعداد صفحات اصل مقاله: 8

نویسندگان:
مجید زارع کاریزی - *دانشجوی کارشناسی ارشد IT، دانشکده فنی و مهندسی، واحد تهران غرب، دانشگاه آزاد اسلامی، تهران، ایران*

سینا دامی - *استادیار گروه کامپیوتر، دانشکده فنی و مهندسی، واحد تهران غرب، دانشگاه آزاد اسلامی، تهران، ایران*

خلاصه مقاله:
سیستم های کنترل صنعتی (ICS) که در کارخانه های صنعتی استفاده میشود، در برابر حملات سایبری آسیب پذیر هستند، بطوریکه این حملات ممکن است آسیب مهلکی به این کارخانه ها وارد کند. سیستمهای تشخیص نفوذ (IDS) ترافیک شبکه ICS را کنترل و فعالیتهای مشکوک را شناسایی میکنند. با این حال، بسیاری از IDSها حملات پیچیده سایبری را نادیده میگیرند، زیرا ایجاد یک پایگاه دادهای کامل از حملات سایبری سخت است، همچنین تشخیص اختلالات عملیاتی هنگامی که با یک مدل پایه ثابت مقایسه میشود، مشکل است. در این مقاله، یک مدل تشخیصی برای جداسازی بسته های نرمال از غیرنرمال ارایه شده است که این مدل توسط یک ماشین یادگیری شدید (ELM) براساس یک پروفایل ارتباطاتی ICS ساخته شده است. مدل مدنظر فقط بازه ها و طول بسته را نشان میدهد . همچنین برای بهبود عملکرد تشخیص نفوذ از شبکه عصبی کانوولوشن (CNN) برای بازنمایی عمیق ویژگی ها بهره گرفته شد. ارزیابی با استفاده از آزمایشهای نفوذ روی پلتفرم آزمایش امنیت سایبری با ویژگیهای عمیق نشان داد، IDS پیشنهادی با کنترل نرخ بسته های حمله پیشبینی شده، با موفقیت حمله های سایبری را شناسایی میکند و عملکرد به مارتب بهتری در مقایسه با مدلهای پایه دارد.

کلمات کلیدی:
سیستم کنترل صنعتی، تشخیص حملات سایبری، بازنمایی ویژگیها، یادگیری عمیق، ELM، CNN