عنوان مقاله:

تشخیص بدافزار اینترنت اشیاء با استفاده از یادگیری عمیق خصمانه

محل انتشار:

اولین کنفرانس بین المللی فناوری اطلاعات، مدیریت و کامپیوتر (سال: 1403)

تعداد صفحات اصل مقاله: 10

نویسندگان:

حامد مظفری – دانشجوی کارشناسی ارشد، دانشکده شبکه و ارتباطات، دانشگاه جامع امام حسین (ع)، تهران

مصطفی عباسی – دانشیار و عضو هیئت علمی ، دانشکده شبکه و ارتباطات، دانشگاه جامع امام حسین (ع)، تهران

خلاصه مقاله:

با گسترش استفاده از تلفن های هوشمند، خطر حملات و گسترش بدافزارهای مخرب در دستگاههای تلفن همراه، به ویژه در سیستم های اندروید، به طور چشمگیری افزایش یافته است . به منظور مقابله با این تهد یدات، از راهکارهای مبتنی بر یادگیری ماشین به عنوان ابزارها ی سیستم های ضد بدافزار استفاده می شود. به همین دلیل ، نویسندگان بدافزار از ویژگی های نمونه های مخرب و نیز نمونه های بی خطر استفاده می کنند تا تفاوت آماری را برای تولید نمونه های خصمانه تقر یب بزنند و الگور یتم های طبقه بندی را فر یب دهند .در مقاله توضیح داده شده است که چگونه مدلهای یادگیری عمیق خصمانه م ی توانند از ویژگی های خاص بدافزارها استفاده کنند و با تحلیل رفتارهای غیرمعمول، حملات را شناسایی کنند. همچنین ، می توانند بهبود پا یداری و دقت تشخیص را در مقابل تغییرات در محیط ها ی اینترنت اشیاء افزا یش دهند. این مقاله تلاش می کند تا راهکارهای نو ین در زمینه تشخیص بدافزار در اینترنت اشیاء با استفاده از یادگیری عمیق خصمانه معرفی کند و امکان پاسخگو یی به چالش های امنیتی پیش رو را با توجه به پیچیدگی محیط اینترنت اشیاء بهبود بخشد.

کلمات کلیدی:

اینترنت اشیاء؛ بدافزار؛ یادگیری عمیق خصمانه ؛ IoT؛ هوش مصنوعی .