بخشی از ترجمه مقاله

عنوان فارسی مقاله :

طرح شناسایی حمله های توزیع شده با استفاده از روش های یادگیری عمقی برای اینترنت اشیا

عنوان انگلیسی مقاله :

Distributed Attack Detection Scheme using Deep Learning Approach for Internet of Things

توجه !

این فایل تنها قسمتی از ترجمه میباشد. برای تهیه مقاله ترجمه شده کامل با فرمت ورد (قابل ویرایش) همراه با نسخه انگلیسی مقاله، اینجا کلیک نمایید.

بخشی از ترجمه مقاله

7. CONCLUSION AND FUTURE WORK

We proposed a distributed deep learning based IoT/Fog network attack detection system. The experiment has shown the successful adoption of artificial intelligence to cybersecurity, and designed and implemented the system for attack detection in distributed architecture of IoT applications such as smart cities. The evaluation process has employed accuracy, the detection rate, false alarm rate, etc as performance metrics to show the effectiveness of deep models over shallow models. The experiment has demonstrated that distributed attack detection can better detect cyber-attacks than centralized algorithms because of the sharing of parameters which can avoid local minima in training. It has also been

demonstrated that our deep model has excelled the traditional machine learning systems such as softmax for the network data classification into normal/attack when evaluated on already unseen test data. In the future, we will compare distributed deep learning IDS for on another dataset and different traditional machine learning algorithms such as SVM, decision trees and other neural networks. Additionally, network payload data, will be investigated to detect intrusion as it might provide a crucial pattern for differentiation.

7-جمع بندی و کار های آتی

در این مقاله، ما یک روش یادگیری عمقی مبتنی بر شبکه های Iot / مه را ارائه کردیم. نتایج نشان داده که می توان از هوش مصنوعی به صورت موفق برای امنیت اینترنتی استفاده کرد و سیستم هایی را برای شناسایی حمله در معماری توزیع شده از برنامه های IoT طراحی و اجرا کرد ؛ این کاربرد ها شامل محیط شهر های هوشمند می باشد. روند ارزیابی برای این الگوریتم بر اساس معیار های صحت، نرخ شناسایی، نرخ اخطار غلط و غیره به عنوان شاخص های عملکرد انجام شده است که این ارزیابی ها نشان دهنده ی کارایی برتر مدل عمقی برای مدل های کم عمق می باشد. آزمایش های ما نشان داده است که شناسایی حمله به صورت توزیع شده می تواند نسبت به الگوریتم های مرکزی ، حمله های اینترنتی را بهتر شناسایی کند زیرا می تواند پارامتر ها را به اشتراک بگذارد و این موضوع مانع شکل گیری مینیموم های محلی در داده های تمرینی می شود. همچنین در این مطالعه نشان داده شده است که مدل عمقی ما نسبت به سیستم های یادگیری ماشینی متداول مانند سافتمکس برای طبقه بندی داده ها به صورت دو طبقه ای نرمال/ حمله در ارزیابی داده های تمرینی جدید، عملکرد بهتری داشته است. در آینده، ما یادگیری عمیق توزیع شده ی IDS را برای یک مجموعه داده ی دیگر و الگوریتم های یادگیری ماشینی متداول مانند SVM ، درخت های تصمیم گیری و دیگر شبکه های عصبی مقایسه می کنیم. به علاوه، داده های حداکثر بار شبکه ها نیز برای شناسایی حمله مورد بررسی قرار می گیرد زیرا این حداکثر بار نیز می تواند الگوهای مهمی برای تمایز بین حالت عادی و حمله شناسایی کند.