سیزدهمین کنفرانس بین المللی نوآوری و تحقیق در علوم مهندسی
گرجستان – تفلیس(۲۰ آبان ماه ۱۴۰۱) -آکادمی بین المللی علوم و مطالعات گرجستان
www.icires.ir
info@icires.ir

یک سیستم تشخیص نفوذ توزیع شده برای شناسایی حملات دیداس در شبکه اینترنت اشیای (IoT) دارای زنجیره بلوکی

شهرزاد شفیعی اردستانی*

دانشگاه آزاد اسلامی واحد تهران جنوب

shahrzadshafiei68@yahoo.com

چکیده

اینترنت اشیا به عنوان تکنولوژی جدیدی برای توسعه ی بسیاری از برنامه های کاربردی مورد نیاز ، ظاهر شده است. اگرچه، این برنامه های کاربردی هنوز بر روی معماری ذخیره سازی متمرکز اجرا شده و چالش های کلیدی زیادی از جمله حریم خصوصی، امنیت و نقطه ی آسیب پذیری مرکزی را دارا هستند. اخیرا، فناوری زنجیره های بلوکی به عنوان ستون فقراتی برای توسعه ی برنامه های کاربردی بر پایه ی اینترنت اشیا پدیدار شده است. زنجیره های بلوکی می توانند به منظور حل مشکلات حریم خصوصی، امنیت و نقطه ی آسیب پذیری مرکزی (ارتباط دهنده ی شخص ثالث) برنامه های کاربردی اینترنت اشیا مورد استفاده قرار گیرند. یکپارچه سازی زنجیره های بلوکی با اینترنت اشیا می تواند برای اشخاص و جامعه سودمند باشد. هرچند، تهاجم نقض سرویس توزیع شده (DDoS) بر استخر استخراج در ۲۰۱۷، خط گسله ای اساسی در میان شبکه ی اینترنت اشیای دارای زنجیره ی بلوکی را نمایان کرد. علاوه بر این، این برنامه اطلاعات بسیار زیادی را تولید می کند. یادگیری ماشینی (ML) به دلیل ارائه ی استقلال کامل در آنالیز داده های بزرگ و قابلیت تصمیم گیری، به عنوان ابزاری تحلیلی استفاده می شود. بنابراین، به منظور پرداختن به چالش هایی که پیشتر ذکر شد، این پژوهش سیستم تشخیص نفوذ توزیع شده ی (IDS) جدیدی با به کارگیری رایانش در مه برای شناسایی تهاجم های DDoS در مقابل استخر استخراج در شبکه ی IoT دارای زنجیره ی بلوکی را ارائه می دهد. عملکرد توسط آموزش الگوریتم جنگل تصادفی (RF) و یک

سیستم بهینه شده ی تقویت درخت گرادیان (XGBoost) بر گره های محاسبات مه توزیع شده، مورد سنجش قرار می گیرد. سودمندی مدل ارائه شده در ارزیابی با استفاده از مجموعه ای حقیقی از داده های مبتنی بر IoT، به عبارت دیگر BoT-IoT که شامل تهاجم های اخیر یافت شده در شبکه ی IoT دارای زنجیره ی بلوکی است. نتایج بیان می کنند که XGBoost برای تشخیص حملات باینری و الگوریتم جنگل تصادفی برای شناسایی حملات چندگانه عملکرد بهتری دارند. به طور کلی، در مورد گره های محاسباتی مه توزیع شده، RF نسبت به XGBoost زمان کمتری را برای آموزش و آزمایش به خود اختصاص می دهد.

کلیدواژگان

زنجیره ی بلوکی، حمله ی دیداس، رایانش در مه، اینترنت اشیا (IoT)، سیستم تشخیص تهاجم، استخر استخراج

مقدمه

اینترنت اشیا (IoT) به عنوان فناوری جدید که با پیشرفت اینترنت، خودش را با زندگی روزمره ی ما ادغام کرده، ظهور کرده است. برنامه های بر پایه ی IoT از جمله مدیریت زنجیره ی تامین، بهداشت و درمان و سیستم مدیریت هویت مبتنی بر RFID به طور مستقیم باعث ارتقای افراد و جامعه می شوند [۱۴]. زیربنای فناوری از طریق ترکیب محاسبه ی ابری و یادگیری ماشینی، برای تجزیه و تحلیل داده ها و مدل سازی نوید دهنده شده است [۳۴]. پیشرفت در حوزه ی توسعه ی مبتنی بر IoT موجب رشد بخش های مختلفی می شود. هرچند، برنامه ی ساخته شده توسط سیستم IoT بیشتر بر روی ذخیره سازی متمرکز و معماری کامپیوتر کار می کند [۲۲، ۶]. مدل ذخیره سازی متمرکز دارای نقص های امنیتی و حریم خصوصی بسیاری است. مدل کارکردی زیربنایی دارای محدودیت هایی برای تسهیل توسعه ی سیستم مبتنی بر IoT در آینده ی نزدیک است [۳۷]. از این رو، برای رسیدگی به این