

روشی برای کشف قوانین وابستگی در پایگاه داده‌های زمانی با استفاده از

گراف رابطه و الگوی تقویتی

دکتر محمد قاسم زاده
دانشگاه یزد، دانشکده برق و کامپیوتر
mghasemzadeh@yazduni.ac.ir
دکтор محمد حسین سرابی
دانشگاه اصفهان، دانشکده برق و کامپیوتر

در دو دهه قبل توانایی های فنی بشر برای تولید و جمع آوری داده‌ها به سرعت افزایش یافته است. بنظر کلی استفاده همگانی از وب و اینترنت ما مواجه با حجم زیادی از داده و اطلاعات می‌کند. این رشد اینفجاری در داده‌های ذخیره شده، نیاز مبرم وجود تکنولوژی های جدید و اینزارهای خودکاری را ایجاد کرده که به انسان یاری رسانند تا این حجم زیاد داده را به اطلاعات و داشت تبدیل کند. داده کاوی به عنوان یک راه برای این مسائل مطرح می‌باشد. داده کاوی را می‌توان عمل استخراج اطلاعات پنهان در یک پایگاه داده بزرگ تعریف کرد. داده کاوی به تحلیلگران برای پیدا کردن الگوهای روابط بین داده‌ها کمک می‌کند. یکی از مهمترین زمینه‌های داده کاوی کشف قوانین وابستگی یا Association Rules mining می‌باشد که هدف از آن یافتن قوانین والکوهای پنهان در بین حجم زیادی از داده‌ها است. همچنین چگونگی کاوش در بین داده‌های که حاوی اطلاعات زمانی هستند به عنوان یک مسأله مهم در امر داده کاوی مطرح است. از آن جایی که بعضی از اقلام داده در کل پایگاه داده به وفور تکرار نصی‌شوند، در صورتی که در یک بازه زمانی دارای درجه پشتیبانی (support) بالایی هستند، Temporal Association Rules mining به کشف قوانین موجود در یک بازه زمانی در پایگاه داده می‌پردازد. یکی از مسلسل مهم در زمینه کاوش در داده‌های زمانی چگونگی تقسیم بدی داده به بازه‌های زمانی می‌باشد. در این مقاله با ارائه روشنی که از الگوی تقسیم برای مشخص کردن بازه‌های زمانی استفاده می‌کند و ترکیب آن با روشنی که از گراف رابطه بین اجرای پایگاه داده استفاده می‌کند به استخراج قوانین موجود در این بازه‌های زمانی پرداخته می‌شود.

تشخیص نفوذ به کمک سیستم‌های چندعامله مبتنی بر اوتوماتاهاي یادگیر

فرزان اطمیح

دانشکده مهندسی کامپیوتر و فناوری اطلاعات
دانشگاه صنعتی امیرکبیر
تهران ایران

abtahi@aut.ac.ir

در این مقاله، یک مدل سلسله مرافقی از عامل‌های مبتنی بر اوتوماتا یادگیر برای تشخیص نفوذ‌های از نوع انکار سرویس پیشنهاد می‌گردد. در مدل پیشنهادی، هر عامل دارای یک اوتوماتا یادگیر است که پرداختهای مدل را تکه‌تکه کرده و آن‌ها را با توجه به بازخوردهای که از محیط دریافت می‌کنند بفرزند برای مدل رسانند. در مدل ارائه شده، مسلسله تشخیص نفوذ بهصورت یک مسئله دست‌بندی دو کلاسه مطرح می‌گردد. برای آموخت و آزمایش این مدل، از KDD99 مجموعه داده‌های استفاده شده که یک مجموعه داده استاندار برای کاربردهای امنیتی می‌باشد. از این‌ها نشان می‌دهند که سیستم تشخیص نفوذ پیشنهادی، در مقایسه با نادرست برخورد نداراست.

واژه‌های کلیدی: تشخیص نفوذ، حملات DoS، سیستم‌های چندعامله، اوتوماتاهاي یادگیر