



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

گراف رابطه و الگوی تقویمی

دکتر محمد قاسم زاده

پروانه رضایت

دانشگاه بزرگ، دانشگاه برق و کامپیوتر

دانشگاه بزرگ، دانشگاه برق و کامپیوتر

m.ghasemzadeh@yazduni.ac.ir

Parvaneh.rezavat@gmail.com

دکتر محمد حسین سرائی

مژگان شبان زاده

دانشگاه صنعتی اصفهان، دانشگاه برق و کامپیوتر

دانشگاه اصفهان، دانشگاه کامپیوتر

در دو دهه قبل توانایی های فنی بشر برای تولید و جمع آوری داده‌ها به سرعت افزایش یافته است. بطور کلی استفاده همگانی از وب و اینترنت ما را مواجه با حجم زیادی از داده و اطلاعات می کند. این رشد انفجاری در داده‌های ذخیره شده، نیاز مبرم وجود تکنولوژی های جدید و ابزارهای خودکاری را ایجاد کرده که به انسان یاری رسانند تا این حجم زیاد داده را به اطلاعات و دانش تبدیل کند. داده کاوی به عنوان یک راه حل برای این مسائل مطرح می باشد. داده کاوی را می توان عمل استخراج اطلاعات پنهان در یک پایگاه داده ی بزرگ تعریف کرد. داده کاوی به تحلیلگران برای پیدا کردن الگوها و روابط بین داده ها کمک می کند. یکی از مهمترین زمینه‌های داده کاوی کشف قوانین وابستگی یا Association Rules mining می باشد که هدف از آن یافتن قوانین و الگوهای پنهان در بین حجم زیادی از داده‌ها است. همچنین چگونگی کاوش در بین داده‌هایی که حاوی اطلاعات زمانی هستند به عنوان یک مساله مهم در امر داده کاوی مطرح است. از آن جایی که بعضی از اقلام داده در کل پایگاه داده به وفور تکرار نمی شوند، 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 می پردازند. یکی از مسائل مهم در زمینه کاوش در داده‌های زمانی چگونگی تقسیم بندی داده ها به بازه های زمانی می باشد. در این مقاله با ارائه روشی که از الگوی تقویمی برای مشخص کردن بازه های زمانی استفاده می کند و ترکیب آن با روشی که از گراف رابطه بین اجزای پایگاه داده استفاده می کند به استخراج قوانین موجود در این بازه های زمانی پرداخته می شود.



تشخیص نفوذ به کمک سیستم های چندعامله مبتنی بر اتوماتاهای یادگیر

فرناز ابیطبی

دانشگاه مهندسی کامپیوتر و فناوری

اطلاعات

دانشگاه صنعتی امیرکبیر

تهران ایران

mmeybodli@aut.ac.ir

abtahhi@aut.ac.ir

در این مقاله، یک مدل سلسله مراتبی از عامل های مبتنی بر اتوماتای یادگیر برای تشخیص نفوذهای از نوع انکار سرویس پیشنهاد میگردد. در مدل پیشنهادی، هر عامل دارای یک اتوماتای یادگیر است که پارامترهای مدل را نگهداری کرده و آن ها را با توجه به بازخوردهایی که از محیط دریافت می کنند به روز می رسانی. در مدل ارائه شده، مسئله تشخیص نفوذ به صورت یک مسئله دستبندی دوکلاسه مطرح می گردد. برای آموزش و آزمایش این مدل، از مجموعه داده های KDD99 استفاده شده که یک مجموعه داده استاندارد برای کاربردهای امنیتی می باشد. آزمایش ها نشان می دهند که سیستم تشخیص نفوذ پیشنهادی، در مقایسه با سیستم های مشابه، از عملکرد مناسبی از لحاظ سرعت، نرخ تشخیص و نرخ خطای مثبت نادرست برخوردار است.

واژه های کلیدی: تشخیص نفوذ، حملات DoS، سیستم های چندعامله، اتوماتاهای یادگیر