عنوان مقاله:
سیستم تشخیص نفوذ به شبکه مبتنی بر داده کاوی ا لگوی رفتار

محل انتشار:
کنفرانس ملی امنیت اطلاعات و ارتباطات (سال: 1389)

تعداد صفحات اصل مقاله: 5

نویسندگان:
حسین جلالی فراهانی - *عضو هیئت علمی دانشگاه آزاد اسلامی واحد ماهشهر گروه کامپیوتر*

علی دقایقی - *مدیریت فناوری اطلاعات و ارتباطات شرکت ملی حفاری ایران اهواز*

بابک فخار - *عضو هیئت علمی دانشگاه آزاد اسلامی واحد ماهشهر گروه کامپیوتر*

خلاصه مقاله:
با توجه به افزایش روزافزون شبکه های کامپیوتری وو جود اطلاعات بسیار مهم در آنها حفاظت از این اطلاعات در برابر حملات و خرابکاریها اهمیت بسیار بالایی پیدا کرده است هدف ازارائه این مقاله طراحی یک سیستم های تشخیص نفوذ به شبکه است درایجاد سیستمهای تشخیص نفوذ از روش های مختلف استفاده میشود که یکی از این روشها داده کاوی است فرایندداده کاوی نیز به روشهای متفاوت صورت می گیرد که یکی از این روشها استفاده از الگوریتم بهینهس ازی کلونی مورچه ها ant- miner است سیستم تشخیص نفوذ پیشنهاد شده الگوهای رفتار نرمال در شبکه را دراختیار می گیرد و براساس مقدار انحراف از رفتار نرمال نفوذ را شناسایی می کند این سیستم برمبنای یافتن ناهنجاریها در رفتار کاربران در شبکه ایجاد شده استو شامل دو فاز ادگیری و تشخیص نفوذ است سیستم پیشنهادی برروی داده KDD99 مستخرج از بانک اطلاعات دانشگاه کالیفرنیا ازمایش و نتیجه حاصل نشان از کارایی مناسب در مقایسه با روشهای SVM,C5 , CUP Winner دارد.

کلمات کلیدی:
سیستم تشخیص نفوذ، شبکه های کامپیوتری، داده کاوی، الگوریتم بهینه سازی کلونی مورچه های، قواعد طبقه بندی