عنوان مقاله:
سیستم تشخیص نفوذ پایگاهداده با رویکرد مبتنی بر توصیف در سطح تراکنش و رویکرد مبتنی بر ناهنجاری در سطح میان تراکنش

محل انتشار:
نهمین کنفرانس بین‌المللی انجمن رمز ایران (سال: 1391)

تعداد صفحات اصل مقاله: 6

نویسندگان:
مصطفی دوردیان - *مرکز تحقیقات سیاست علمی کشور- دانشکده مهندسی کامپیوتر و فناوری اطلاعات، دانشگاه صنعتی امیرکبیر، تهران*

حمیدرضا شهریاری - *دانشکده مهندسی کامپیوتر و فناوری اطلاعات، دانشگاه صنعتی امیرکبیر، تهران*

خلاصه مقاله:
امروزه اطلاعات نقش مهمی را در سازمان ها ایفا می نماید. اطلاعات حساس اغلب در پایگاه داده ها ذخیره می شوند. به دلیلافزایش روزافزون اطلاعات در سازمان ها و حساس بودن آنها مکانیزم های قدیمی از قبیل رمزنگاری و کنترل دسترسی نمی توانندسطح اطمینان بالایی را برآورده نمایند. از این رو وجود سیستم های تشخیص نفوذ در پایگاه داده ها امری ضروری به نظر می رسد. دراین مقاله یک سیستم تشخیص نفوذ به منظور شناسایی حملات پایگاه داده در دو سطح تراکنش (تراکنش های غیر مجاز) و میان-تراکنش (ناهنجاری در ارتباط میان تراکنش ها) ارایه می شود. برای این منظور در سطح تراکنش یک رویکرد تشخیص مبتنی برتوصیف تراکنش های مورد انتظار موجود در برنامه های کاربردی پایگاه داده ارایه می شود. سپس در سطح میان تراکنش یک رویکردتشخیص مبتنی بر ناهنجاری با استفاده از داده کاوی براساس استخراج ارتباطات میان تراکنش ها پیشنهاد می شود. از مزیت های اینسیستم نسبت به سیستم های تشخیص نفوذ پایگاه داده ی قبلی می توان به قابلیت این روش در تشخیص حملات در هر دو سطحتراکنش و میان تراکنش و نیز تشخیص بسیاری از حملات تزریق پرس وجو و همچنین تشخیص سوءاستفاده ی داخلی اشاره نمود.آزمایشاتی به منظور ارزیابی میزان درستی عملیات سیستم انجام شده است که نتایج آن از میزان درستی بالای عملکرد سیستمحکایت دارد.

کلمات کلیدی:
تشخیص نفوذ، امنیت پایگاه داده، توصیف، ماشین وضعیت، داده کاوی، قوانین میان تراکنشی