عنوان مقاله:
تشخیص نفوذ در پایگاه داده با استفاده از همبسته سازی رویدادنامه ها

محل انتشار:
پنجمین کنفرانس بین المللی مدیریت فناوری اطلاعات و ارتباطات (سال: 1387)

تعداد صفحات اصل مقاله: 13

نویسندگان:
سیدامید آذرکسب - *دانشجو کارشناسی ارشد هوش مصنوعی دانشگاه آزاد اسلامی قزوین ایران*

سعید شیری قیداری - *دکترای تخصصی کامپیوتر رباتیک استادیار دانشگاه صنعتی امیرکبیر تهران*

خلاصه مقاله:
امروزه سیستم های تشخیص نفوذ به طور قابل ملاحظه ای برای افزایش امنیت شبکه های کامپیوتری مورد استفاده قرار می گیرند حجم بالا و کیفیت پایین رویدادنامه های تولید شده نیاز به پردازش بیشتر این رویدادنامه ها را توجیه میکند مدیران شبکه توانایی ارتباط دادن رویدادنامه ها را به صورت دستی فراهم می آورند اما مشکل اصلی دراین روش فقدان انعطاف پذیری ، زمانبر بودن و نداشتن یک دید عمومی نسبت به رویدادنامه ها می باشد بدون این دید عمومی پیدا کردن ارتباط بین اطلاعات اجزا شبکه و رخدادهایی که ظاهرا غیر اصلی به نظر می رسد ولی از قسمتهای یک تهدید به شمار می روند غیر ممکن است دراین راستا روشهای همبسته سازی رویدادنامه ها با هدف افزایش کیفیت هشدارها و ارایه جمع بندی قابل درک از وضعیت امنیتی جاری به تحلیلگر امنیتی مطرح شده اند دراین مقاله روشی جدید برای همبسته سازی رویدادنامه ارائه می شود که در آن پردازشهای مرکزیت دادن نرمالایز کردن ادغام کردن گردآوری، همبسته سازی، مصور سازی و قابلیت اصلاح و تجدید نظر که از معیارهای اجرایی اصلی یک سیستم تشخیص نفوذ مبتنی بر رویدادنامه های همبسته متمرکز است در پنج مولفه تامین کننده پیش پردازنده، تحلیلگر، ارزیاب و مدیر و کنترل کننده مرکزی پیاده سازی گردیده است نتایج حاصله بیانگر تاثیر به سزای استفاده از همبسته سازی رویدادنامه ها بربهبود سیستم های تشخییص نفوذ می باشد.

کلمات کلیدی:
امنیت کامپیوتر، همبسته سازی رویدادنامه ها، تشخیص تهاجم، تشخیص سواستفاده، تشخیص ناهنجاری، شبکه عصبی خودسازمانده SOM