عنوان مقاله:
استفاده از الگوریتم رمزSerpentبرای رمز نگاری پایگاه داده های رابطه ای

محل انتشار:
دهمین کنفرانس دانشجویی مهندسی برق ایران (سال: 1386)

تعداد صفحات اصل مقاله: 8

نویسندگان:
داود کیمیا - *دانشجوی کارشناسی ارشد مهندسی کامپیوتر، دانشگاه آزاد اسلامی واحد تهر*

علی جعفری مند - *دانشجوی کارشناسی ارشد مهندسی کامپیوتر، دانشگاه آزاد اسلامی واحد تهر*

صالح حافظ قرانی - *دانشجوی کارشناسی ارشد مهندسی فناوری اطلاعات، دانشگاه صنعتی امیرکبیر*

خلاصه مقاله:
اهمیت بانک های اطلاعاتی و کاربرد روزافزون آنها در توسعه سیست مهای اطلاعاتی و نقش حیاتی آنها در تمرکز داد ههها باعث می شودتا پرداختن به امنیت آنها ضروری به نظر برسد. در این مقاله به ارائه روشی برای پنها نسازی داده ها با استفاده از الگوریت مهای رمز و ترکیب آنها به صورتLoose Coupling با پایگاه داده ها می پردازیم. استفاده از این روش باعث می گردد تا کاربران غیر مجاز قادر به دسترسی به داده های مذکور نباشند و در عین حال کاربران مجاز با داشتن کلید و بدون درگیر شدن با جزئیات و پیچیدگ یهای محاسباتی اضافی، به راحتی به داده های خود دسترسی داشته باشند. مزایا و معایب این روش مورد بحث و بررسی قرار می گیرد و پیشنهاداتی ارائه می گردد الگوریتم رمز بلوکیSerpentکه یکی از فینالسیت های مسابقاتAES میباشد، به عنوان نمونه آزمایشی مورد استفاده قرار گرفته است. یک Case Study برای این منظور در نظر گرفته شده و روش پیشنهادی در آن اعمال گردیده است. در انتها نتایج یک نمونه عملی با بکارگیری این الگوریتم ارائه م یگردد

کلمات کلیدی:
امنیت پایگاه داده، پایگاه دادههای رابطه ای، رمزنگاری، رمزهای بلوکی، الگوریتم رمزSerpent

لینک ثابت مقاله در پایگاه سیویلیکا: