مروری بر ارزیابی روش های رمزگذاری و امنیت در پایگاه داده توزیع شده

امام بخش ارباب شهستان[1] ، دکتر احمد فراهی[2]

[1]دانشجوی کارشناسی ارشد، مهندسی کامپیوتر گرایش نرم افزار ، دانشگاه پیام نور واحد تهران شمال ، ایران
Emambakhsharbab@gmil.com

[2]استادیار و عضو هئیت علمی، سازمان مرکزی دانشگاه پیام نور
afaraahi@pnu.ac.ir

چکیده

در این محیط مدرن، استفاده از اینترنت و استفاده از رایانه ها با سرعت بسیار بالا رو به رشد است و استفاده از پایگاه داده نیز با همان سرعت افزایش می یابد. نیاز به امنیت پایگاه داده نیز در این محیط بسیار مهم است، زیرا در هر پایگاه داده فعالیت های آنلاین مورد نیاز است و اگر به هر دلیلی امنیت پایگاه داده به خطر افتاده باشد، این تهدیدی جدی برای اطلاعات حساس و محرمانه خواهد بود. محققان مختلف پایگاه داده روش هایی برای محافظت از فرم پایگاه داده این آسیب پذیری ها ارائه دادند، اما هیچ کدام از این روش ها قادر به محافظت از فرم های پایگاه داده انواع تهدیدات امنیتی نیستند. یکی از محبوب ترین روش ها برای اطمینان از امنیت پایگاه داده، از طریق رمزنگاری است. در این مقاله مورد بررسی و تحلیل قرار می دهیم استفاده از کاتالوگ پایگاه داده ایمن برای ذخیره داده های رمز شده از کاربران در پایگاه داده برای محافظت از اطلاعات در پایگاه داده را مورد ارزیابی قرار می دهند.

واژه های کلیدی

امنیت ، رمزنگاری، تهدیدات، کاتالوگ پایگاه داده امن، معماری

۱-مقدمه

استفاده از اینترنت به بخشی از زندگی روزمره هرکسی تبدیل شده است. خرید آنلاین به چهره جدید برای انجام کسب و کار تبدیل شده است. در این زمان، هنگام استفاده از تمام خدمات قدیمی و جدید، مردم نگران حفظ حریم خصوصی و یکپارچگی اطلاعات کسب و کار خود هستند. به تازگی، حمله به یک وب سایت محبوب که منجر به سرقت تعداد کارت های اعتباری چندین هزار مشتری شد. این نشان می دهد که اگر جزئیات کارت اعتباری یا سایر اطلاعات شخصی به نحوی به سرقت رفته باشد، می تواند برای مشتریان سایت های آنلاین بسیار مضر باشد بنابراین امنیت در آن محیط بسیار مهم است. یک سیستم مدیریت ارتباط پایگاه داده نقش مهمی در کسب و کار جدید بازی می کند. مقدار زیادی از اطلاعات کسب و کار جمع آوری، ذخیره و پردازش می شود، که نیاز به پشتیبانی قویتری از سرور پایگاه داده دارد اگر ما به فعالیت خرید یک مشتری وب نگاه کنیم و اطلاعات را ردیابی کنیم، می توانیم ببینیم که دو مسئله امنیتی مورد توجه قرار گرفته اند. انتقال امن داده ها ، هنگامی که یک مشتری اطلاعات شخصی و محرمانه خود را (به عنوان مثال شماره کارت اعتباری) از طریق مرورگر وب خود ارسال می کند، ذخیره سازی امن و دسترسی به داده ها هنگامی که داده های شخصی و محرمانه مشتری به سرور پایگاه داده وارد می شوند، داده ها باید به گونه ای ذخیره شوند تا دسترسی به این داده ها فقط برای تأیید مردم با پروسه مجوز مناسب باشد . انتقال امن داده ها به خوبی مورد بررسی قرار گرفته و در بازار تجارت الکترونیک امروز پشتیبانی خوبی دارد. تمام مرورگرهای وب و سرورهای وب[1] و [2]پشتیبانی می کنند. شماره کارت اعتباری در حین انتقال از یک مرورگر وب به یک سرور وب از طریق اتصال[3] محافظت می شود. با این حال، هنگامی که داده ها به سرور پایگاه داده وارد می شوند، در نگهداری و پردازش آنها به صورت امن پشتیبانی کافی وجود ندارد. پشتیبانی از رمزنگاری در سیستم مدیریت ارتباط با پایگاه داده بسیار مهم است. پشتیبانی از رمزنگاری یک بعد مهم در امنیت پایگاه داده و افزایش سیاست های امنیتی است. این مکمل دسترسی کنترل و رمزنگاری و کنترل دسترسی هر دو می تواند امنیت اطلاعات محرمانه ذخیره شده در پایگاه داده را افزایش دهد. هنگامی که ما در مورد ادغام پشتیبانی رمزنگاری به سیستم مدیریت ارتباط با پایگاه داده فکر کردیم، سه رویکرد کلی وجود دارد. سرویس رمزنگاری شخص ثالث می تواند توسط سرور پایگاه داده مشورت شود و تنها تغییرات جزئی در سمت سرور وجود دارد. یک مجموعه کامل از پایه های رمزگذاری اولیه به سرور پایگاه داده به عنوان مجموعه ای از دستورات اسکیوال جدید، همراه با زمینه کنترل و اجرای لازم برای اطمینان از اینکه این دستورات اسکیوال جدید می تواند ایمنی این رویکرد وظیفه بسیار سخت تر از آن است که از لحاظ پیاده سازی، اما این کار در بلندمدت ترجیح داده می شود.

برای تطابق با نیاز فوری برای ارتقاء امنیت، تنها یک زیر مجموعه کوچک از ابتدای رمزگذاری در سرور پایگاه داده یکپارچه می شود، بر

[1] Secure Socket Layer
[2] Security Layer Security
[3] Secure Socket Layer