رمزنگاری پنهان داده در سمپاد ارتقاءیافته PostgreSQL

مرکز آپا دانشگاه صنعتی شریف
https://cert.sharif.edu

سرآغاز

در فضای تبادل اطلاعات برای امنیت داده‌ها با سه مسئله مواجه هستیم:

- امنیت داده‌های در انتقال،
- امنیت داده‌های ذخیره شده،
- امنیت داده‌های در حال پردازش.

از آنجایی که پایگاه‌داده‌ها به عنوان انباره‌ای برای ذخیره‌سازی داده‌ها و مدیریت آن‌ها به شمار می‌روند، تأمین امنیت آن‌ها از نیازمندی‌های اصلی در حوزه‌ی امنیت داده‌ها در ذخیره‌سازی است. تاکنون مدل‌های کنترل دسترسی گوناگونی برای حفاظت از اطلاعات بر اساس خط‌مشی‌های موجود در سیستم‌های مدیریت پایگاه‌داده‌ها مطرح شده‌اند. این در حالی است که راه‌های متفاوتی نیز برای عبور غیرمجاز از این خط‌مشی‌ها و دسترسی غیرمجاز به داده‌ها وجود دارد.

سرقت رسانه ذخیره‌سازی، مثال دیگری از تهدیدات ممکن است که می‌تواند امنیت داده‌های مجتمع شده در پایگاه داده را به مخاطره اندازد. بر این اساس، رمزنگاری داده‌ها یکی از مکانیزم‌هایی است که در کنار برخی از مکانیزم‌های دیگر برای افزایش ضریب امنیتی در سیستم‌های مدیریت پایگاه‌داده‌ها به کار می‌رود.

یکی از مکانیزم‌های موجود برای محافظت از داده‌های ذخیره‌شده در رسانه‌ی ذخیره‌سازی سمپاد (سیستم مدیریت پایگاه داده)، رمزنگاری پنهان داده است که امروزه توسط اکثر سمپادهای تجاری رایج همچون اوراکل، DB2 و SQL Server پشتیبانی می‌شود. در رمزنگاری پنهان داده، همانطور که از نام آن مشخص است عملیات رمزنگاری از دید کاربر کاملا پنهان است و کاربر بدون هیچ محدودیتی پرس‌وجوهای خود را اجرا می‌نماید؛ درحالی که داده‌ها به صورت رمز شده در رسانه ذخیره‌سازی، ذخیره می‌شوند.

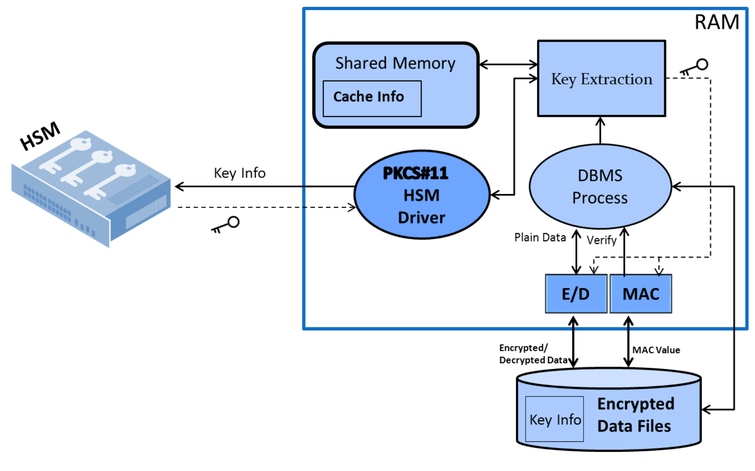
در سمپاد ارتقاء یافته PostgreSQL که توسط مرکز آپا دانشگاه صنعتی شریف ایجاد شده است، رمزنگاری پنهان داده با قابلیت‌هایی قابل مقایسه و حتی فراتر از سایر سمپادهای تجاری فراهم شده است.

ویژگی‌های اولیه سمپاد ارتقاءیافته

- ✓ نصب آسان بر روی توزیع‌های مختلف لینوکس مانند ubuntu، debian و centos،
- ✓ نصب آسان در محیط گرافیکی یا خط فرمان،
- ✓ واسط گرافیکی کاربرپسند برای مدیریت رمزنگاری پنهان داده در سمپاد،
- ✓ تضمین محرمانگی و صحت داده‌های هدف،
- ✓ مدیریت جامع و یکپارچه‌ی کلیدهای رمزنگاری،
- ✓ افزودن دستورات SQL جدید و به‌روز رسانی برخی از دستورات موجود SQL با هدف پشتیبانی از ویژگی‌های رمزنگاری پنهان‌داده،
- ✓ افزودن دیدها و جداول سیستمی جدید به سمپاد با هدف پشتیبانی از ویژگی‌های رمزنگاری پنهان‌داده و نمایش اطلاعات مربوط به رمزنگاری پنهان داده به کاربران.

معماری کلی

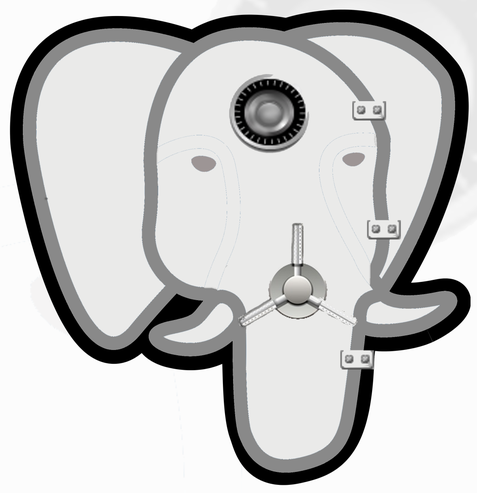
شمای کلی سمپاد ارتقاءیافته.



تضمین محرمانگی و صحت

سمپاد ارتقاءیافته PostgreSQL مورد نظر، موارد زیر را برای تضمین محرمانگی و صحت تامین می‌کند.

- ✓ پشتیبانی از رمزنگاری پنهان داده در سطح ستون و جدول،
- ✓ تضمین صحت داده‌های موجود در جداول،
- ✓ پشتیبانی از انواع داده‌های رمزشده عددی و رشته‌ای،
- ✓ پشتیبانی از الگوریتم‌های رمزنگاری مختلف،
- ✓ پشتیبانی از الگوریتم‌های تضمین صحت مختلف،
- ✓ رمز فایل‌های پشتیبان،
- ✓ رمز فایل‌های رویدادنگاری،
- ✓ رمزفایل‌های موقت میانی،
- ✓ رمز و تضمین صحت جداول سیستمی (کاتالوگ)،
- ✓ پشتیبانی از تعریف شاخص بر روی جداول رمزشده یا جداول حاوی ستون رمز شده،
- ✓ رمز جداول شاخص.



مدیریت کلید در سمپاد ارتقاءیافته

مدیریت کلید از طریق موارد زیر در سمپاد ارتقاءیافته PostgreSQL اجرایی شده است.

- ✓ استفاده از معماری دولایه مدیریت کلید،
- ✓ شاه‌کلید رمزنگاری برای رمزکلید جداول،
- ✓ کلید جداول برای رمز داده‌های جداول،
- ✓ مدیریت کلید در مؤلفه امنیتی نرم‌افزاری یا سخت‌افزاری (HSM)،
- ✓ امکان پشتیبان‌گیری و بازیابی کلیدهای جداول و شاه‌کلیدها،
- ✓ امکان تجدید کلید رمزنگاری جداول،
- ✓ امکان تجدید شاه‌کلید رمزنگاری

امکانات موجود در واسط گرافیکی

برخی از امکانات سمپاد ارتقاءیافته PostgreSQL:

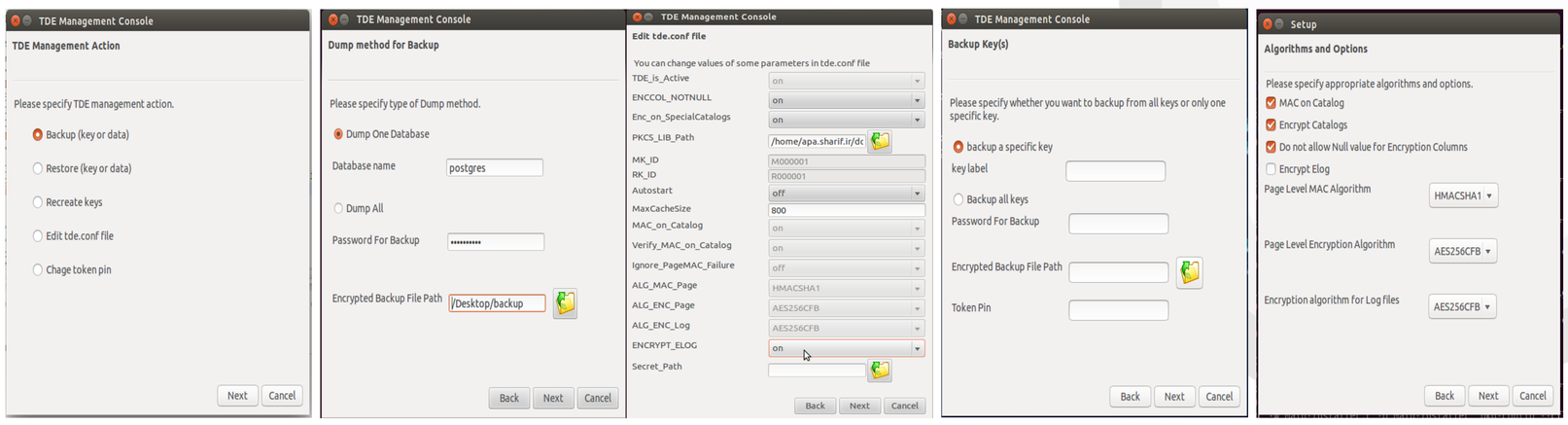
- ✓ پشتیبان‌گیری از داده‌ها و کلیدهای رمزنگاری،
- ✓ بازیابی داده‌ها و کلیدهای رمزنگاری،
- ✓ تجدید کلیدهای رمزنگاری،
- ✓ پیکربندی رمزنگاری پنهان داده در سمپاد ارتقاءیافته،
- ✓ تغییر کلمه عبور مؤلفه‌ی امنیتی ذخیره‌کننده‌ی کلید.

مقایسه با سمپاد اوراکل

در بحث رمزنگاری پنهان داده، سمپاد ارتقاءیافته حتی از سمپاد تجاری اوراکل (که در رمزنگاری پنهان داده نسبت به سایر سمپادها کاملتر است)، نیز پیشی می‌گیرد. مقایسه سمپاد ارتقاءیافته توسط مرکز آپا دانشگاه صنعتی شریف با سمپاد اوراکل به لحاظ امکانات رمزنگاری پنهان داده در جدول زیر آمده است.

ویژگی	ORACLE	
رمزنگاری با ریزدانگی ستون و جدول	✓	✓
رمز فایل‌های پشتیبان و فایل‌های میانی	✓	✓
رمز فایل‌های رویدادنگاری	عدم پشتیبانی در برخی از فایل‌های رویدادنگاری همچون audit log و elog	✓
رمز جداول سیستمی	×	✓
تضمین صحت در سطح فایل، ردیف و جداول سیستمی	عدم تضمین صحت داده‌ها در هر سطر از جدول و در جداول سیستمی	✓
شاخص بر روی داده‌های رمز شده	پشتیبانی از شاخص تنها برای عملگر تساوی	✓
پشتیبانی از کلید خارجی بر روی ستون رمزشده	×	✓

چند نما از رابط کاربری



درباره مرکز آپا دانشگاه صنعتی شریف

مرکز آگاهی‌رسانی، پشتیبانی و امداد در حوزه‌ی افتا (آپا) شریف، با رویکرد استفاده از نیروهای دانشگاهی در سال ۱۳۸۶ جهت خدمت به صنعت کشور و تقویت پیوند دانشگاه و صنعت، در دانشکده مهندسی کامپیوتر دانشگاه صنعتی شریف راه‌اندازی گردید. آپا معادل مفهومی واژه Computer Emergency Response Team (CERT)، یک تیم خدماتی است که هدف اصلی آن ارائه خدمات امنیتی، با محور مدیریت و تحلیل حوادث، و آسیب‌پذیری‌ها در فضای تبادل اطلاعات به سازمان‌ها و کاربران است. مرکز آپا دانشگاه صنعتی شریف به عنوان مکمل مرکز امنیت داده و شبکه شریف فعالیت‌های خود را در جهت ارائه خدمات امنیتی به کاربران و سازمان‌ها دنبال نموده است.

در طی ۱۴ سال فعالیت مرکز آپا دانشگاه صنعتی شریف پروژه‌های مشاوره و تحقیقاتی متعددی به اجرا رسیده و یا در حال اجرا است که از اهم آن‌ها می‌توان به طراحی و پیاده‌سازی سامانه‌های: تلسکوپ آی‌پی برای شبکه ـ کشف شبکه‌های بات ـ فروچاله نام دامنه ـ تحلیل بدافزارهای جمع‌آوری‌شده از شبکه تله‌عسل ـ کنترل دسترسی چندسطحی سمپاد بومی ـ و کشف شواهد جرائم رایانه‌ای مبتنی بر ترافیک شبکه اشاره کرد. همچنین این مرکز، فعالیت به‌سزائی در آگاهی‌رسانی، پشتیبانی و امداد در خصوص امنیت انواع سمپادها در سطح کشور و ارائه خدمات رسیدگی رخداد و حملات امنیتی به سازمان‌ها و شرکت‌های مختلف داشته است.

آدرس مرکز: تهران، خیابان آزادی، دانشگاه صنعتی شریف، دانشکده مهندسی کامپیوتر، طبقه‌ی ۵، مرکز آپا دانشگاه صنعتی شریف
تلفن و نمابر: ۷ـ ۶۶۱۶۶۶۷۵ وب‌سایت: https://cert.sharif.edu