数据加密存储系统
产品白皮书

格尔软件股份有限公司
上海格尔安全科技有限公司
北京格尔国信科技有限公司
http://www.koal.com

信息更新

本文档仅用于为渠道代理商或最终用户提供信息，并且随时可由格尔公司更改或撤回。

信息反馈

格尔软件股份有限公司欢迎您通过尽可能多的渠道向我们提供尽可能多的信息，您的意见和问题都会得到我们的重视和妥善处理，请将反馈信息投递到地址：上海市静安区江场西路299弄中环时代广场4号楼6楼。

服务热线：400-021-8870

传 真：021-62327015

公司网址 http://www.koal.com

目录

1 前言

1.1 研制背景

我国在大数据、云计算、人工智能、物联网、 5G 等新技术带动下的数字经 济发展过程中，数据已经成为国家和企业的重要资产和战略资源，多来源多类 型的数据集中整合与综合应用带来了爆发式增长，与此相伴的是数据过度采集 和使用、数据泄漏等安全风险日益凸显，同时还面临严峻的国际信息安全和国 内泄漏风险等挑战。如何有效的进行数据的安全防控成为国家、单位和个人所 面临的严峻挑战。采用数据加密技术实现数据的保护是很重要的技术手段，可 以保证数据的机密性，防止用户访问数据库导致重要敏感数据丢失以及因为数

据文件丢失导致的重要数据信息泄露。

针对网络内处理重要数据项的应用系统，提供应用免改造字段级数据加密存储功能，数据加解密在应用内完成，明文数据不会传出应用系统或者数据库之外；支持保留格式加密，支持对密文数据进行模糊查询功能；实现重要数据存储安全防护保障，满足国家关于数据安全及密码应用的相关要求，提升数据安全防护能力。

1.2 行业法规要求

国家制定了与数据安全隐私保护相关的法案法规，以保证用户的敏感数据不会被泄露，有些行业对于敏感数据的保护也有着不同的行业标准和规范，如： 等级保护： 数据保密性要求采用密码技术保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。

密评、密测：应用和数据安全需要保证重要数据完整性。

中华人民共和国数据安全法：建立数据安全治理体系，提高数据安全保障能力。

1.3 名词解释

本白皮书的名词解释有：

表格 1-1 产品相关名词解释

名词	解释
SM4	是中华人民共和国政府采用的一种分组密码标准，是一种分组密码算法

SM2	椭圆曲线公钥密码算法是我国自主设计的公钥密码算法

2 产品概述

数据加密存储系统一款对数据库中存储的敏感数据进行加密保护的产品，该产品采用国产密码算法实现数据的透明加解密，在写入数据时自动加密，在读取 数据时自动解密，确保敏感数据在数据库中全程处于密态，防止敏感数据的外泄。

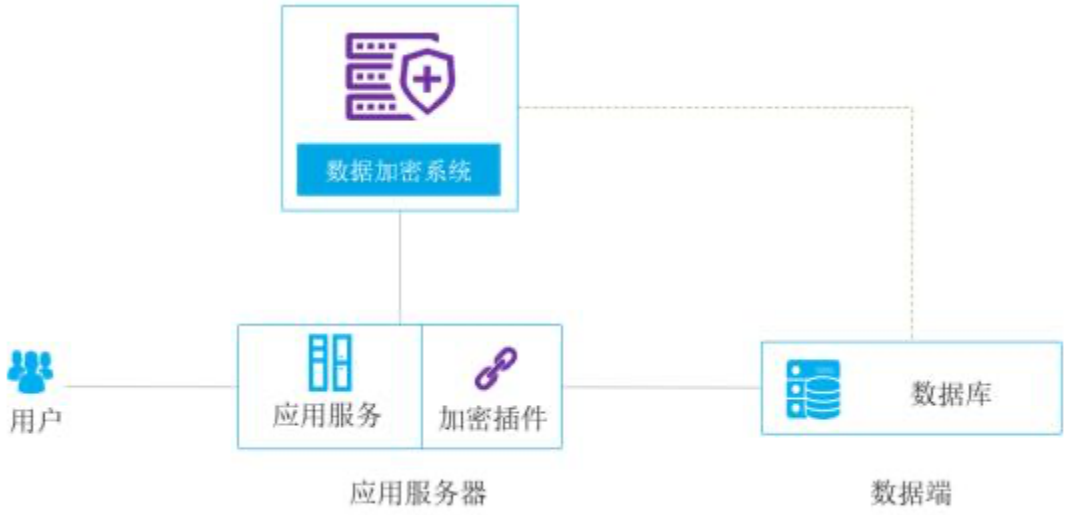

图 2-1 数据加密存储系统逻辑示意图

2.1 产品形态

序号	模式	产品形态	适用场景
1	硬件模式	硬件设备	适用于本地机房部署或者云环境机房托管方式部署的场景。

2	纯软模式	纯软件，支持云化虚机部署	适用于采用虚拟机或云化部署的场景。 比如阿里云、华为云、腾讯云等云化环境。

第一种应用模式：产品以硬件的形式部署， 可以快速进行应用集成。

第二种应用模式： 产品以纯软件的形式部署在云平台上，支持分布式部署，可以部署到阿里云、华为云、腾讯云等云化环境。

2.2 应用环境要求

1、数据加密存储系统需要访问待加密的数据库。

2、应用服务器需要访问数据加密存储系统。

3、产品支持IPv6，允许在加密机主服务器之间、加密机与数据库服务器之间以IPv6方式进行通信。

3 产品功能

3.1 数据源管理

提供数据源的图形化管理、支持非国产数据库，如：Oracle系列、SQL Server系列、My SQL系列以及mariadb等、DB2等、以及国产数据库，如：Gbase 8a、华为GaussDB系列、达梦系列、人大金仓系列、TDSQL系列数据库、海量数据库所有版本。

3.2 敏感字发现

敏感数据发现能力，提供可视化的敏感数据发现，支持任务方式配置敏感数据识别、提供多种数据识别算法，包括：自定义发现算法、代码表、正则表达式等，支持敏感数据变化跟踪。

3.2.1 内置发现算法

数据域发现能力开箱即用，内置丰富的发现算法，如：姓名、地址、电话、公司、身份证号、卡号等。

3.3 数据加密密钥管理

3.3.1 多加密算法支持

支持国密算法SM系列、国际加密算法 DES、3DES、AES128、3DES等加密算法标准。支持SM4 ECB、CBC、OFB、CFB、GCM、CCM等多种算法模式等加密算法，支持基于SM4算法的各种类型的格式保留加密算法，包括身份证格式保留加密、护照号格式保留加密、电子邮箱格式保留加密、数字格式保留加密。

3.3.2 密钥管理

系统的密钥管理采用web图形化方式配置，支持密钥管理和加密策略、以及数据加密的管理功能。

密钥管理系统采用三层密钥体系，包括根密钥、模块主密钥和工作密钥；支持密钥的生命周期管理，支持安全服务组件实现对密钥的管理，包含加密密钥生成、分配、备份和恢复，密钥不出设备（卡）；支持从第三方密钥管理获取密钥，支持密钥轮换，支持国密算法。

采用密码卡时，支持由密码卡根据周围环境（噪音、温度）生成随机数，保护根密钥。

3.3.3 密钥更换

提供对已经加密的数据更换加密的密钥，更换密钥后会按照新密钥对数据进行加密。

3.3 数据加密策略管理

支持图形化方式配置加密策略，提供对数据字段项设置加密规则，提供数据库列级加密， 并支持对不同字段列设置不同的密钥和加密算法。支持对数据库列名等元数据进行混淆以隐藏真实数据库元数据信息。

加密策略配置时，支持CHAR、VARCHAR、VARCHAR2、LOB、JSON、NUMBER等数据类型的加密。

3.4 数据透明加解密

系统提供免改造方式加密，支持在运维场景和应用系统应用场景中通过安装插件等方式进行数据加密，业务应用时以明文方式访问数据库,实现高效数据访问。

对于java应用系统，加密系统支持字段级的切面脱敏能力，同时保持数据库数据不做修改。

数据加解密

在应用内完成，明文数据不会传出应用系统或者数据库之外。在加密解密过程中，加密系统出现异常，不影响业务系统的正常运行。

支持数据库中原有的存储过程、函数、视图等在加密后数据库上正常运行，无需进行代码改造，运行结果与明文保持一致。

3.4.1 加密初始化

提供图形化的数据加密配置，可以对指定数据表列的全部数据进行一次性加密进行加密，加密初始化时使用与字段加密配置一样的加密算法和密钥。

3.4.2 入库数据加密

对配置了加密规则的字段，数据入库时对数据进行加密。支持对数据库列名数据进行加密以隐藏真实数据库元数据信息。

3.4.3 出库数据解密

对配置了加密规则的字段，数据出库时对数据进行解密。

3.4.4 查询条件加密

对配置了加密规则的字段作为查询条件时，对条件值进行加密后进行查询。

3.4.5 加密数据还原

对于已经加密的数据，提供加密数据还原功能，可以将加密数据还原成明文数据。

3.5 数据脱敏

系统提供动态脱敏功能，支持自定义脱敏策略，可以进行图形化脱敏策略配置，支持脱敏配置的产生、生效、失效等全生命周期管理。

3.6 访问控制

系统对接入加密解密能力的应用端提供访问控制的功能，只有授权应用才可进行加密解密。支持将合法用户与应用系统绑定，提供基于IP策略的访问控制方式，同一用户只能通过指定的应用系统访问密文数据，非授权的用户使用命令行、管理工具等其他任何方式均无法访问密文数据。

3.7 备份管理

提供对全部密钥和加密策略进行导出备份和恢复的功能。加密不影响数据库自身的数据库恢复、备份、同步等操作，备份结果支持以文件方式进行存储。支持额外的离线数据恢复工具，保证极端情况下数据也能恢复到原始状态，支持加密策略以文件方式导入应用系统，实现数据的加密解密，保证数据的高可用性。

系统的加密策略和恢复支持系统跨版本升级和恢复。

3.8系统安全

3.8.1 三权分立

系统支持三权分立，可以设定系统管理员、安全管理员和安全审计员。

3.8.2 日志审计

系统提供完善的日志记录，提供应用端访问系统访问的详细记录，记录访问发生的时间、主体、客体、内容等信息。

支持对操作日志的日志审计功能，并提供基于HMAC技术保护操作日志的完整性。

4 产品特点

数据加密存储系统支持国密算法，采用三级密钥体系，实现敏感信息传输和存

储的机密性保护，系统性能高，应用改造成本低。

4.1 不改数据服务使用习惯

不改变数据服务调用方的使用习惯，不需要特定客户端，只需要在系统设置即可实现敏感数据的透明加解密，应用系统改造几乎无成本。

用户在使用加密数据时不仅支持密文精准查询，还支持模糊查询、关联查询。支持密文计算功能，可对密文数据直接进行函数运算，运算结果与明文保持一致，不影响实际应用的计算结果。

支持密文数据不解密可视化运维，具有权限的运维者可通过管理工具以查阅明文的方式查看密文，但密文本身并没有解密为明文。只对需要查看的数据进行临时解密。

通过专门的运维管理工具，在授权的情况下，支持运维人员以明文数据管理方式直接管理密文数据，不改变原有数据管理习惯。

4.2 防止拖库

数据库数据加密存储，即使通过数据库客户端工具连接数据库，看到的仍然是密文数据，拷贝和导出数据都不会导致敏感数据外泄，数据导出和爬取内存得到的也不是明文，防止敏感数据外泄，将数据管理权与所有权彻底分离。

4.3 支持高系统压力

实现应用侧分布式密码计算，不增加数据库服务器的负担。支持HA高可用方式部署，支持主、从互备、并且支持第三方负载均衡。

4.4 高强度数据安全

应用授权访问，应用侧数据信源加密。提供透明加解密模式，不对原有应用系统产生影响，无需在数据库服务器部署任何代理程序，不对原数据库有任何侵入，可实现数据库加密功能快速上线。支持基于主密钥保护下的密钥备份和恢复，保证系统的安全性和可靠性。

5 产品价值

5.1 实现敏感信息机密性保护

通过加密技术，实现敏感数据的机密性保护，防止数据泄露，数据破坏。支持应用免改造字段级加密，支持保留格式加密，加密后的数据以密文形态存储。

5.2 防止外部攻击和内部违规操作

系统对敏感数据进行加密存储，防止由于外部黑客攻击或内部违规操作导致的敏感信息泄露。

5.3 安全合规

满足等保、密评对数据的机密性保护的要求。

5.4 支持广泛的使用场景

采用多种方案支持主流开发语言，包括 Java、C、Python等不同开发语言。

支持Linux系列操作系统，包括：centos、UOS V20、银河麒麟V10等。

6部署方式

加密系统支持以旁路方式进行部署。实施时不需要改变业务系统及数据库系统的网络拓扑结构，实施后不会影响业务系统对数据库系统的访问。加密系统上线只需提供系统对数据库的网络访问权限以及业务系统对加密系统的网络访问权限。

具有Web图形化管理界面，易于安装及加密策略部署。

支持系统的快速部署和卸载、具备快速、准确的整体拆除能力，并提供加密数据还原的能力，实现系统快速还原。

7产品参数

外观规格	2U
网络接口	4个 10/100/1000Mb自适应接口

	1个千兆管理网口 支持扩展2/4个万兆光口
电源	双模块冗余电源，支持断电保护备份等机制
CPU	16核国产化CPU
内存	≥128G
硬盘	SAS硬盘1TB*1，支持存储空间扩展
加解密性能	SM4 加解密速率为 40Gbps
数据库服务性能	相同业务压力时加密后应用系统、数据库服务整体性能损失相比加密前不超过10%，不影响业务运行。

8技术支持

格尔软件股份有限公司

电 话：021-62327010

传真： 021-62327015

地址：上海市江场西路 299 弄 5 号中铁时代广场 4 楼 6 楼

邮编： 200436