文章编号:1671－251X(2012)07－0007－04
陈运启,张翼.煤矿瓦斯监控系统关键数据加密算法的研究与实现[J].工矿自动化,2012(7):7-10.

煤矿瓦斯监控系统关键数据加密算法的研究与实现

陈运启[1,2], 张翼[1,2]

(1.中煤科工集团重庆研究院,重庆 400039;
2.瓦斯灾害应急信息技术国家重点实验室,重庆 400039)

摘要:为了防止煤矿瓦斯监控系统中关键数据被篡改,保证数据安全,提出一种在SQL Server 2008数据库中利用对称加密算法对重要字段进行加密,并使用密钥和解密函数还原数据的方法。字段被对称加密后,任何对该字段数据的更改操作都需要得知密钥,并使用解密函数才能实现,从而有效地防止了对关键数据的非法操作,保护了敏感数据。实际应用证实了关键数据加密算法的有效性。

关键词:煤矿;瓦斯监控;数据保护;数据加密;对称加密算法;SQL Server 2008
中图分类号:TD76 文献标识码:A 网络出版时间:2012－07－02 09:43
网络出版地址:http://www.cnki.net/kcms/detail/32.1627.TP.20120702.0943.003.html

Research of Critical Data Encryption Algorithm of Gas Monitoring System of Coal Mine and Its Implementation

CHEN Yun-qi[1,2], ZHANG Yi[1,2]

(1.Chongqing Research Institute of CCTEG., Chongqing 400039, China. 2.State Key Laboratory of Gas Disaster Emergency Information Technology, Chongqing 400039, China)

Abstract: In order to prevent critical data of gas monitoring system of coal mine from tampering and ensure data security, the paper proposed a method of using symmetric encryption algorithm to encrypt important field in database of SQL Server 2008 and restore data by key and decryption function. Any changes to the encrypted data cannot be achieved unless knowing the key and using the decryption function, so as to effectively prevent the illegal operation of critical data and protect sensitive data. Practical application confirmed validity of the critical data encryption algorithm.

Key words: coal mine, gas monitoring, data protection, data encryption, symmetric encryption algorithm, SQL Server 2008

0 引言

瓦斯灾害是煤矿最为严重的灾害之一,瓦斯突出和瓦斯爆炸不仅造成了国家财产损失,还经常导致大量的人员伤亡。瓦斯监控系统可监测井下瓦斯的活动情况,对于确保煤矿安全生产有着非常重大的社会与经济意义。瓦斯监控系统中采集、存储的井下环境参数是事故发生后确定事故原因最基本、最真实的资料,可用于判断事故的性质及责任级别,因此瓦斯监控系统应保证监控数据的真实性,防止数据被随意读取或篡改[1-3]。最新的国家煤矿监控系统标准[4]中对此也有明确的要求与规定。本文提出一种在SQL Server 2008数据库中利用对称加密算法对重要字段进行加密,并使用密钥和解密函数还原数据的方法。

1 煤矿瓦斯监控系统简介

煤矿瓦斯监控系统主要设备包括矿用环网平台

收稿日期:2012－04－26
基金项目:国家重点基础研究发展计划(973计划)资助项目(2005CB221506);中煤科工集团重庆研究院项目(CK2010)
作者简介:陈运启(1984－),男,安徽萧县人,助理工程师,硕士,主要研究方向为煤矿安全监测及矿山自动化。E-mail:chen.yun.qi@qq.com

设备、监控主机、监控分站、各类传感器、数据采集解析服务器、数据库服务器、Web 服务器、Web 终端等。系统整体架构如图 1 所示。

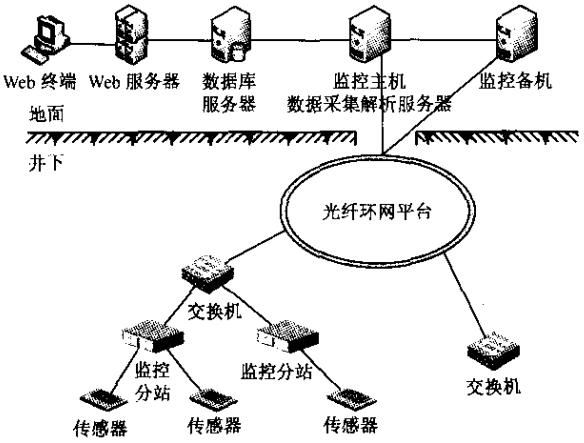

图 1 煤矿瓦斯监控系统整体架构

SQL Server 2008 作为微软数据库平台中的一个最新版本，提供了强大的搜索、查询、数据分析、报表、数据整合功能，其吞吐量和数据挖掘功能较以前版本也有了很大提高，完全满足瓦斯监控系统的要求，因此系统采用 SQL Server 2008 作为数据库服务器。

2 数据库加密技术

数据库加密的目的是保护存储于数据库内的数据，防止数据泄露和非法访问。数据加密后以密文方式存储并在密态方式下工作，以得到有效保护。在没有密钥和解密函数的情况下，即使用户非法入侵系统或盗得了数据库文件，也不能获取或篡改所需数据，从而确保了数据的安全。

2.1 数据库加密粒度

按照数据库的结构层次，数据库加密粒度可分为数据库级、表级、记录级、字段级以及数据项级[5-6]。根据不同的应用需要，可以选择合适的加密粒度。

数据库级加密粒度：加密对象是整个数据库，对所有的用户数据表、系统数据表、索引、视图、存储过程、函数等都进行加密处理。这种加密方法比较简单，只需要对存储在磁盘中的相应数据库文件进行加密处理即可，一个数据库只对应一个密钥，密钥数量少，管理方便。同时，数据库的数据共享性高，被多个用户和应用共享使用时，需要接受大量的随机访问。但多数情况下，用户访问数据库时，只需检索符合条件的很少一部分记录，若采用数据库级加密粒度则要对整个数据库进行解密，对系统性能产生极大影响。

表级加密粒度：加密对象是数据库中的表。通常来说，数据库包含多个表，只需要对其中一些包含敏感信息的表进行加密，以保护它们的安全性。若数据库采用表级加密粒度，则访问时只需要对特定的表进行解密，与采用数据库级加密粒度相比，系统性能有一定的改善。

记录级加密粒度：加密对象是数据表中的记录，将记录中各字段值连接在一起进行加密处理，加密后输出一列字符串。与数据库级和表级加密粒度相比，这种加密粒度更细，灵活性更好。但在只需访问记录中的某一部分数据（字段）时，要对整条记录进行解密，从而带来了不必要的性能开销。

字段级加密粒度：加密对象是记录中的某个字段。字段级加密是一个很好的选择，因为现实中一些重要和敏感的信息往往出现在关系中的某些列，只需对这些重要内容进行加密即可，普通数据则没有必要加密。

数据项级加密粒度：加密对象是某些记录中的某个字段的值，它是数据库加密的最小粒度。数据项级加密方法更为灵活，它与字段级加密的实现方式相似，但其密钥管理更加复杂。

2.2 数据加密算法

根据加密密钥与解密密钥是否相同，加密算法分为对称加密算法和非对称加密算法。对称加密即加密和解密使用相同的密钥，常用的对称加密算法有数据加密标准（DES）、三重数据加密标准（3DES）、高级加密标准（AES）等。而非对称加密算法又称为公开密钥加密算法，它使用 2 个具有数学关系的不同密钥加密和解密数据，这 2 个密钥分别称为私钥和公钥，常用的非对称密钥加密算法有 RSA 公钥算法等。对称加密算法的速度比非对称加密算法快几十甚至几百倍，其对系统性能的影响较小，因此在 SQL Server 2008 中使用较多[7-8]。

3 SQL Server 2008 加密机制

SQL Server 2008 加密机制如图 2 所示。服务主密钥（Service Master Key）是一个规定 SQL Server 中所有密钥和证书的密钥。它是 SQL Server 在安装期间自动创建的对称密钥。数据库主密钥（Database Master Key）是所有密钥、证书和数据库中数据的根加密对象。每个数据库只有一个数据库主密钥。证书（Certificates）是一个数字签名语句，它将公钥的值绑定到拥有对应私钥的人员、设

备或服务的标识上，其包含主题的公钥、主题的标识符信息、有效期等信息。由SQL Server 2008创建的自签名证书遵循 X.509 标准，并支持 X.509 v1 字段。对称密钥(Symmetric Keys)和非对称密钥用于对数据库中的数据进行加密和解密。

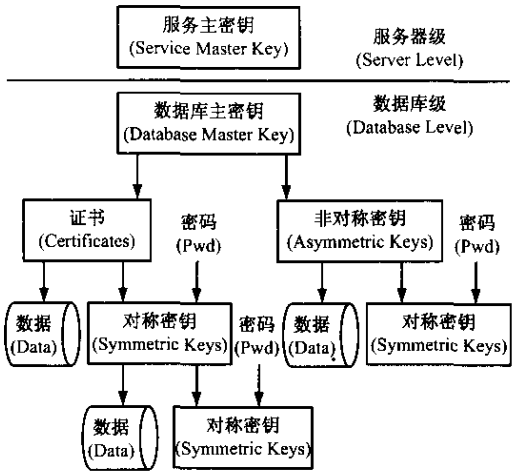

图 2　SQL Server 2008 加密机制

4　瓦斯监控系统关键数据加密的实现

瓦斯监控系统采集到的井下环境参数如瓦斯浓度、一氧化碳浓度、温度、通风参数等是非常重要的数据[4,9]，为了防止对这些数据篡改，需要对数据进行加密，然后再存储到数据库(DB_GasMonitor)中。每个监测设备都对应实时监控数据和历史监控数据，下面以实时数据表 (TB_Realdata)(见表 1)为例[10]，介绍关键数据加密的实现过程。

表 1　实时数据表(TB_Realdata)

列名	数据类型	备注
pointId	INT	测点编号(FK)
realValue	Nvarchar	加密后的实时值
Address	Nvarchar	测点地址
timeStamp	DATETIME	采集时间
⋮	⋮	⋮

步骤 1：创建数据库主密钥。

```
USE DB_GasMonitor
CREATE MASTER KEY
ENCRYPTION BY PASSWORD=@password
```

步骤 2：创建数据证书，其私钥被数据库主密钥加密。

```
CREATE CERTIFICATE DB_GasMonitorCert
WITH SUBJECT='DB_GasMonitor Certificate',
START_DATE='2010-01-01',
EXPIRY_DATE='2020-12-31'
```

步骤 3：创建对称密钥，并用证书对其进行加密。

```
CREATE SYMMETRIC KEY DB_GasMonitorKey
WITH ALGORITHM = DESX
ENCRYPTION BY CERTIFICATE DB_GasMonitorCert
```

步骤 4：打开对称密钥，插入加密数据。

```
OPEN SYMMETRIC KEY DB_GasMonitorKey
DECRYPTION BY CERTIFICATE DB_GasMonitorCert
INSERT INTO TB_Realdata(pointId, realValue) VALUES
(@pointId, EncryptByKey(Key_Guid('DB_GasMonitorKey'),
@realvalue))
CLOSE SYMMETRIC KEY DB_GasMonitorKey
```

步骤 5：解密数据。

```
OPEN SYMMETRIC KEY DB_GasMonitorKey
DECRYPTION BY CERTIFICATE DB_GasMonitorCert
SELECT pointId, CAST(DecryptByKey(realvalue) AS
VARCHAR) AS realValue FROM TB_Realdata
CLOSE SYMMETRIC KEY DB_GasMonitorKey
```

若使用“SELECT pointId, realValue FROM TB_Realdata”语句向 TB_Realdata 表中插入实时数据(见表 2)，得到的结果是没有任何意义的密文，如图 3 所示。只有通过步骤 5，使用证书打开密钥，再用解密函数解密才能看到实际数据。由于解密函数是数据库自带函数[9]，它的使用基本上不影响数据库效率。

表 2　插入的实时数据

pointId	realValue	…
3302538	0.17	…
3302539	0.11	…
3302540	0.05	…
3302541	0.05	…

	pointId	realValue
1	3302538	0x00CB2D721C91004CAA58C95953FA51B9010000000E89D19...
2	3302539	0x00CB2D721C91004CAA58C95953FA51B9010000000F17050E...
3	3302540	0x00CB2D721C91004CAA58C95953FA51B901000000003B34D51...
4	3302541	0x00CB2D721C91004CAA58C95953FA51B9010000000FC2AF38...

图 3　未使用密钥查询得到的数据

5　结语

在 SQL Server 2008 数据库中对关键字段进行对称加密后，任何对这些字段数据的更改操作都需要在得知密钥，并使用解密函数才能实现，从而有效防止了对关键数据的非法操作，很好地保护了敏感数据。采用关键数据加密技术的煤矿瓦斯监控系统在淮北、山西等煤矿的应用证实了加密算法的有效性。

文章编号:1671-251X(2012)07-0010-04
聂伟峰,余韵,贺琪. 与无线自组网相结合的配电通信网络延伸方案[J]. 工矿自动化,2012(7):10-13.

与无线自组网相结合的配电通信网络延伸方案

聂伟峰[1], 余韵[1], 贺琪[2]

(1. 华北电力大学电气与电子工程学院, 北京 102206;
2. 湖南省电力公司长沙电业局, 湖南 长沙 410000)

摘要:针对配电通信网络存在网络盲区的问题,提出一种与无线自组网相结合的配电通信网络延伸方案;介绍了常用的无线自组织网络、WIA网络结构及性能分析、配电通信网络延伸方案的三层结构。该方案利用无线自组织网络的多跳性和自组织性,实现了盲区终端数据的回传。实际应用结果表明,该方案不但成本低、功耗低,且具有数据传输时延短、安全性高等优势。

关键词:配电通信网络; 网络通信盲区; 网络延伸; 无线自组网络; WIA
中图分类号:TD655.3 文献标识码:A 网络出版时间:2012-07-02 09:44
网络出版地址:http://www.cnki.net/kcms/detail/32.1627.TP.20120702.0944.004.html

An Extension Scheme for Distribution Communication Network Combined with Wireless Ad Hoc Network

NIE Wei-feng[1], YU Yun[1], HE Qi[2]

(1. Department of Electrical and Electronic Engineering of NCEPU., Beijing 102206, China.
2. Changsha Electric Power Supply Bureau of Hunan Electric Power Corporation, Changsha 410000, China)

Abstract: In allusion to problem of blind area of distribution communication network, the paper proposed an extension scheme for distribution communication network combined with wireless ad hoc

收稿日期:2012-04-24
基金项目:国家科技重大专项基金资助项目(2010ZX03006-005-01)
作者简介:聂伟峰(1984-),男,内蒙古赤峰人,硕士研究生,研究方向为电力通信。E-mail:nieweifeng2008@126.com

参考文献:

[1] 王佳琦,王宇奇. 我国一次能源供应结构的系统分析[J]. 科技与管理,2011,13(1):62-65.
[2] 张宇. 煤矿事故应急救援能力评价体系的构建研究[D]. 大连:大连交通大学,2011.
[3] 李波. 煤矿安全监控系统分析与设计[D]. 北京:北京邮电大学,2009.
[4] 国家质量监督检验检疫总局计量司,国家安全生产监督管理总局规划科技司,国家煤矿安全监察局科技装备司,等. 矿山安全计量常用法律法规及标准[M]. 北京:中国计量出版社,2007.
[5] 汪培芬. 数据库加密技术的研究与实现[D]. 南京:南京理工大学,2008.
[6] 张超. 数据库加密技术在SQL Server 2008中的应用分析[J]. 宿州教育学院学报,2010,13(4):140-143.
[7] 范瑛. 基于SQL Server 2008安全数据库服务器的构建[J]. 甘肃联合大学学报:自然科学版,2009(增刊2):43-44,56.
[8] 杜立健,唐晓燕,李守荣. 几种信息加密算法的比较研究[J]. 网络安全技术与应用,2006(8):88-89.
[9] FAROULT S, ROBSON P. SQL语言艺术[M]. 温昱,靳向阳,译. 北京:电子工业出版社,2008.
[10] 李文艳,陈运启. 煤矿安全监控系统中模拟量查询算法优化[C]//国际信息技术与应用论坛论文集,昆明,2010:242-244.
[11] 勾成图,张璟,李军怀. 海量数据分页机制在Web信息系统中的应用研究[J]. 计算机应用,2005(8):1926-1929.