

基于 DAS 模式的电子商务系统模型设计与研究

黄显文^{1,2}, 王志晓¹, 施海滨¹

(1 中国矿业大学 计算机科学与技术学院, 江苏 徐州 221116; 2 龙煤集团 鹤岗分公司团委, 黑龙江 鹤岗 154101)

摘 要: 用 xml 半结构化数据文件系统代替普通 B/S 模式的传统数据库, 设计了 DAS(Data As a Service)模式下的电子商务模型, 主要包括客户端数据加密、服务器密钥管理和数据服务提供商对 xml 加密数据的查询处理等。结合 xml 索引技术与基于层次的 Dewey 编码搜索方法实现用户订单 xml 加密数据的查询处理。该方案在保证系统的安全性、稳定性前提下, 大大减小了系统的维护成本, 提高了系统的性能和运行效率, 有利于促进企业的效益。

关键词: DAS; XML; 加密; 数据查询; 电子商务

中图分类号: TP311

文献标识码: A

文章编号: 1000-7180(2011)10-0071-04

Design and Research of an E-Commerce System Model Based on DAS

HUANG Xian-wen^{1,2}, WANG Zhi-xiao¹, SHI Hai-bin¹

(1 School of Computer Science & Technology, China University of Mining and Technology, Xuzhou 221116, China;
2 The Council of the Communist Youth League of Hegang Branch, Longmei Group Co., Ltd, Hegang 154101, China)

Abstract: Substituted XML Semi-Structured Data Files System for the traditional database based on common B/S mode, and designed an E-Commerce System Model based on DAS (Data As a Service), which mainly included Client Data Encryption, Server Key Management and the query processing of XML enciphered data by data service provider etc. The query processing of XML enciphered data in user orders are implemented by XML index technology combined with Dewey coding. It is shown that, on the premise of security and stability, the proposed solution can greatly reduce the maintenance cost of system, and improve its performance and operation efficiency, which is beneficial to promote the enterprise benefit.

Key words: DAS; XML; encryption; data query; e-commerce

1 引言

DAS 概念基本上提倡这样的观点: 随着面向服务体系结构 (Service-Oriented Architecture, SOA) 的产生, 它包含对数据所在地数据存取的标准处理, 而与数据所在地的平台无关紧要。DAS 开始于这样的想法: 可发生在数据质量能被认证的地方, 净化 and 丰富数据并将其提供给不同的系统, 应用或用户, 各自在组织内部或在网络上。

该模式已被应用于关系数据库系统和 XML^[1] 数据库系统等领域^[2]。数据库服务提供商 (Data Base Service Provider, DBSP) 这一角色开始在许多企业级应用计算方案中出现。企业或组织不再需要专门

维护自己的数据中心, 而是把数据库系统的管理和维护工作全部委托给 DBSP, 将其作为一种服务来使用, 这种方案在性能和成本上具有诸多的优势^[3]。

DAS 模式的基本结构如图 1 所示, 它主要由客户端、服务器和数据服务提供商三部分组成。数据拥有者本身不再自行管理数据, 而是将其数据存放在一个专业管理与维护第三方平台。而通常情况下, 第三方并不是完全被信任的, 故在其上存放的客户端数据均已经过加密。

2 模型的建立及 xml 数据存取方案设计

引入 DAS 模式, 实行数据外包技术, 减少了服务器的工作量, 解决了网络拥塞和服务器瓶颈现象。

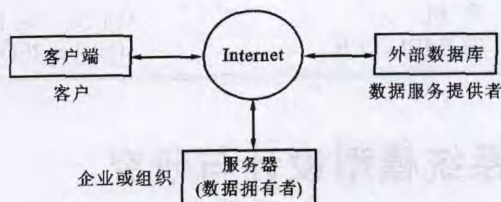


图1 DAS模式的结构

结合XML数据流通方案设计的电子商务系统模型如图2所示,主要包括订单数据、产品数据、查询消息、查询结果、用户密钥的传送或转发等数据活动^[4]。

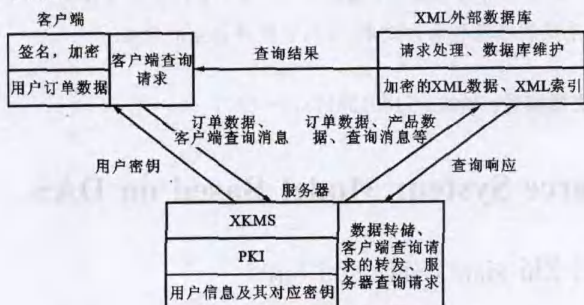


图2 DAS模式下的XML数据存取方案示意图

该XML数据流通方案的基本原理^[5]:一是除服务器对客户端数据查询外,xml订单数据的加密与解密全部在客户端执行;二是在网络上传输的客户数据都是经过加密的;三是xml数据外包给数据服务提供者,而且它是存储和管理加密后的xml数据;四是服务器只负责管理用户信息、用户密钥及数据与消息的转发等。

Internet、电子商务的飞速发展,也带来各种各样的安全威胁,如:网络传输的信息易被窃听、截获、篡改;假冒实体身份非法获取关键资源访问;伪造电子邮件、否认电子商务交易活动等。该模式下将数据中心外包,似乎带来了更大的安全隐患,为了解决网络安全问题,在网络上传输的数据和在数据服务提供者存储的客户数据均是经加密的数据,而加/解密密钥仍然保存在服务器,是否发送密钥给客户端由服务器来决定。这样一来,就解决了DAS模式下的数据安全威胁。

3 方案实现

对该模型中主要数据流通与管理部件的实现技术如下:

(1)用户xml订单数据的传送:客户端产生订单数据data后,自身生成加密密钥对(加密公钥 $key_{pub-client}$ 与加密私钥 $key_{pri-client}$),向服务器申请用户

密钥(key_{user})并传送加密公钥 $key_{pub-client}$ 而自己保留私钥 $key_{pri-client}$,服务器验证用户身份后生成对称的用户密钥对 key_{user} ,用加密公钥对用户密钥进行加密后 $ENCRYPT-key_{pub-client}(key_{user})$ 传送给客户端。客户端则可用加密私钥解密获得用户密钥,即 $DECRYPT-key_{pri-client}(ENCRYPT-key_{pub-client}(key_{user}))$ 。客户端获得用户密钥 key_{user} 后,对xml订单数据进行签名、加密 $ENCRYPT-key_{user}(SIGNATURE-key_{pri-client}(data))$,发送至服务器。服务器接收到订单数据后,将其交由数据服务提供者进行整合。

C#实现如下:

①创建CspParameters对象,指定密钥容器的名称,生成RSA密钥(客户端实现)。

客户端产生RSA密钥后,将其公钥传递至服务器,用于加密AES密钥。

②使用RijndaelManaged类生成AES对称密钥,该密钥将被用来对XML元素进行加密(服务器实现)。加密前的AES密钥Key与IV见图3,加密后的AES密钥Key与IV见图4。

加密前的Key:82	82	47	22	250	172	44	55	214
227	145	69	38	207	94	46	88	35
238	29	136	23	230	155	191	152	108
247	93	111						
解密前的IV:25	35	190	167	161	104	51	70	91
121	194	133	107	140	182	219		

图3 加密前的AES密钥Key与IV

加密后的Key:52	243	121	251	1	51	148	69	1
221	192	176	216	41	185	195	57	135
23	68	119	155	116	119	186	44	102
16	121	96	81	152	116	117	168	123
204	168	136	178	91	97	95	102	39
69	181	198	237	118	7	115	115	181
233	289	148	94	223	177	24	189	158
23	145	28	52	174	214	134	80	190
23	242	248	132	121	45	198	27	143
91	83	198	215	58	142	36	223	117
186	6	201	189	102	81	119	149	227
24	165	118	28	78	184	188	213	87
72	176	86	66	16	200	91	159	133
解密后的IV:45	54	251	213	134	51	68	74	283
237	99	27	14	12	130	42	231	167
16	135	219	120	137	2	46	223	142
210	185	226	104	128	201	184	204	125
58	72	184	22	98	203	79	143	73
36	157	244	0	239	55	235	30	57
65	173	94	234	16	241	149	26	81
93	74	22	63	104	113	107	68	222
97	166	153	248	196	201	17	105	135
7	211	39	0	124	171	50	179	242
188	4	186	32	48	141	117	41	223
68	246	23	230	26	288	165	210	32
153	225	98	115	70	154	55	131	33

图4 加密后的AES密钥Key与IV

③服务器生成的AES对称密钥经加密并传输至客户端,RSA解密(客户端实现)。解密后的AES密钥Key与IV见图5。

解密后的Key:82	82	47	22	250	172	44	55	214
227	145	69	38	207	94	46	88	35
238	29	136	23	230	155	191	152	108
247	93	111						
解密后的IV:25	35	190	167	161	104	51	70	91
121	194	133	107	140	182	219		

图5 解密后的AES密钥Key与IV

④解密对称密钥后,将对应的Key与IV赋给新建的RijndaelManaged对象。这样,就可以在客户端运用服务器生成的AES对称密钥对XML加密

了,而该对称密钥由服务器保存和管理,而客户端使用一次后丢弃。

⑤运用上述获取的 AES 密钥对 XML 订单数据加密,Encrypt(XmlDocument Doc, string ElementName, SymmetricAlgorithm Key)。

⑥将加密后的 xml 订单数据存入文件,经服务器传至数据服务提供者,最终与 XML 数据库整合。对于加密后的 XML 文档仍然保持着 XML 文档的树型结构,称为子树替代不变性,这一点给加密文档的各种操作带来了便利。

(2)客户端数据查询:从是否查询加密数据角度分为两种:一是查询条件中不包含被加密部分的内容,而且客户不需要查看被加密部分的信息,此类查询称为普通查询(Query1);二是查询条件包含已被加密部分的内容,或条件中不包含已被加密的内容,而需要查看被加密信息,此类称为加密数据查询(Query2)。从查询信息的粒度不同又分为子树查询与节点查询:子树查询是对用户对应子树的整体信息查询,记为 Query3;节点查询是对用户对应子树中的部分信息查询,记为 Query4。Query1 自始至终都不涉及对 xml 数据的解密,故也不需要向客户端传送用户密钥,它属于普通 xml 文档的数据查询,只是此类查询结果子树中剔除或者隐蔽那些加密子节点。在此主要从加密数据查询 Query2 方面进行讨论。

Query2 主要过程描述如下:

客户端发出查询消息:SendMessage(“Query1: 条件 1;条件 2;…”),服务器首先对用户身份进行验证,如果通过验证则转发查询消息至数据服务提供者,并记录该用户已通过验证。

数据服务提供者接收到来自服务器的查询消息后,执行如下 XML 加密数据查询过程:

- 1//检索 XML 加密数据文档的索引表,找出该用户第一个子树节点,目的是获得该节点所在层次。
2. 截取最后所获 sDewey 的最后一位,即得到父节点 dewey 编码 faDewey.
3. 对父节点所有的子节点进行遍历,找到所有该用户子节点以及允许查询得其他用户节点的非加密部分,同时将符合条件的节点组织起来,建立结果子树 XML 文件。

继而获得其下一兄弟节点 XmlNode nextNode = currNode.NextSibling;直到对所有子节点循环结束。

(3)数据服务提供者的工作:总的来说是对 xml 数据库的管理、维护及查询处理,它主要包括用户 xml 订单数据片段的整合、修订或退货 xml 数据片

段的处理、对应 xml 索引的修改与维护、xml 文档的查询处理以及 xml 数据库的撤销、恢复等日常事务的处理。订单整合是将用户的 xml 订单数据片段融合到系统 xml 数据库文件中,即在 xml 数据库树结构中添加新的子节点,随后将其对应的索引编码添加至 xml 索引列表文件中,xml 索引表结构如表 1 所示,包含用户编号、加密节点 dewey 码以及该加密节点的父节点 dewey 码。数据服务提供者存放 xml 加密数据的文档结构如图 6 所示,该树型结构的 dewey 编码只需对未加密节点编排,而加密节点的子节点不必编排 dewey 码。

表 1 xml 加密数据的文档索引表

userNumber	加密节点 Dewey 码	该子树的父节点
123	0. 0. 6	0. 0
123	0. 1. 6	0. 1
111	0. 2. 6	0. 2
111	0. 3. 6	0. 3
...	...	...

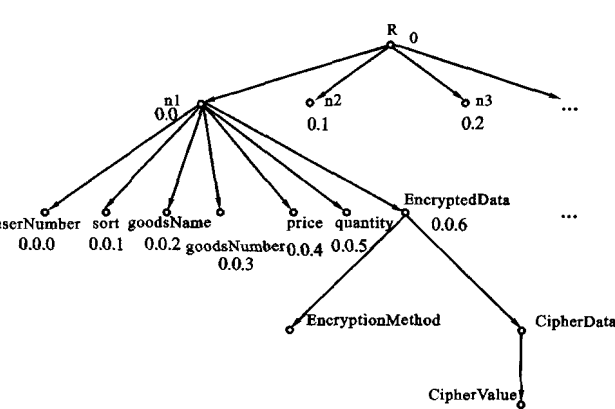


图 6 xml 加密数据的文档树结构

(4)服务器对用户密钥的管理:服务器才是数据库真正的主人,只有它才有权利存取所有数据,其中包含各用户的加密数据。服务器管理着所有用户的用户密钥,也就是 xml 文档的加/解密密钥。每个用户对应一个密钥,而密钥由用户注册并经服务器认证后由服务器产生,继而保存在服务器,而客户端不保存密钥。当该用户上传或下载查询结果时,根据需要,服务器验证其身份后便将密钥发送至对应用户加密或解密 xml 数据,用户密钥索引表结构如表 2 所示,它包含了用户及其对应密钥的相关信息。

表 2 用户密钥索引表

userNumber	userInfo	密钥名称	密钥 Key 值
123	Address, CertifyDate, ...	Key_User_123	Byte[Key_User_123]
111	Address, CertifyDate, ...	Key_User_111	Byte[Key_User_111]
...	...	...	...

相对于普通的 B/S 模式,该模式具有诸多优点,主要体现在安全性好、效率高;减轻了工作量并降低了成本。

4 结束语

设计了一种 DAS 模式下 xml 数据存取方案^[6],通过将 xml 数据库外包给数据服务提供者管理的方法实现。数据服务提供者存储加密数据的措施解决了数据外包的安全性威胁,而它专业的 xml 数据库管理模式给系统带来了稳定性,同时大大减小了维护成本和服务器负荷。本方案的设计,对电子商务类网站、xml 技术以及数据外包技术的发展有着积极的推动作用。

参考文献:

- [1] 孟小峰,王宇,王小峰. XML 查询优化研究[J]. 软件学报,2006,10(17):2069—2086.
- [2] Ravi Chandra Jammalamadaka, Sharad Mehrotra. Querying encrypted XML documents, Database engineering and applications symposium[C]// IDEAS '06. 10th In-

ternational. India, Delhi, 2006:129—136.

- [3] Hakan Hacigümüs, Bala Iyer, Mehrotra S. Providing database as a service [C]//Proc of ICDE. Washington, DC, USA: IEEE Computer Society, 2002.
- [4] Hui Wang, Laks V S Lakshmanan. Efficient secure query evaluation over encrypted XML databases[C]//Proc of VLDB 2006. New York: ACM, 2006.
- [5] Mykletun E, Tsudik G. Incorporating a Secure Coprocessor in the Database—as—a—Service Model [C]// Innovative Architecture for Future Generation High—Performance Processors and Systems. USA: Washington, 2005.
- [6] 孔令波,唐世渭,杨冬青,等. XML 信息检索中最小子树根节点问题的分层算法[J]. 软件学报,2007,18(4):919—932.

作者简介:

黄显文 男,(1982—). 研究方向为数据挖掘。

王志晓 男,(1979—),博士,讲师。研究方向为人工智能、数据挖掘。

施海滨 男,(1987—). 研究方向为图像处理、数据挖掘。

(上接第 70 页)

- [3] Hughes G, Bultan T. Automated verification of access control policies [D]. USA: Computer Science Department, University of California, 2004.
- [4] Sloman M. Policy—driven management for distributed systems[J]. Journal of Network and Systems Management, 1994, 2(4):333—360.
- [5] Dunlop N, Indulska J, Raymond K. Dynamic conflict detection in policy—based management systems[C]// Proceedings of the 6th International Enterprise Distributed Object Computing Conference (EDOC), Lausanne,

Switzerland: IEEE, 2002:15—26.

- [6] Ernesto damiani. A fine—grained access control system for XML documents[J]. ACM Transactions on Information and System Security, 2002,5(2):169—202.

作者简介:

张爱娟 女,(1979—),博士研究生。研究方向为信息安全、分布式 GIS。

高井祥 男,(1960—),博士生导师。研究方向为大地测量、矿山 GIS。