DOI:10.13196/j.cims.2015.03.026

面向产业链协同 SaaS 平台多源信息动态集成安全技术研究

潘　华,王淑营,孙林夫,吕　瑞
(西南交通大学 CAD 工程中心,四川　成都　610031)

摘　要:针对产业链协同平台与联盟企业信息动态集成的过程中身份认证、访问控制等可能存在的安全隐患,建立了多源信息动态集成安全的数学模型,提出了面向产业链协同 SaaS 平台多源信息动态集成安全解决方案。该方案利用 Hash 算法生成数字摘要,实现了 Web 服务传输过程中数据的完整性,利用非对称加密技术、数字签名技术实现了 Web 服务网络传输保密性和发送信息的不可抵赖性。以产业链协同平台协作企业查询车辆库存信息为例,通过平台协作企业集成向导安装的身份认证、注册服务信息过程中数据的完整性及保密性验证,验证了该方案的可用性和有效性。

关键词:产业链;软件即服务;多源信息;动态集成;数据安全;加密技术
中图分类号:TP393　　**文献标识码**:A

Multi-source dynamic integration security for SaaS collaborative platform of industrial chain

PAN Hua, WANG Shu-ying, SUN Lin-fu, LYU Rui
(Center of CAD Engineering, Southwest Jiaotong University, Chengdu 610031, China)

Abstract: For the possible security hidden trouble during process of industry chain collaboration platform and enterprise information integration, a mathematical model on multi-source information dynamic integration security was established. A multi-source information dynamic integration security solution of Software as a Service (SaaS) collaborative platform oriented to industrial chain was proposed. The digital abstract was generated with Hash algorithm to realize the integrity of the data in the transmission process of Web service. By using asymmetric encryption technology and digital signature technology, Web service network transmission security and non repudiation of sending message were realized. Taking cooperation enterprise inventory information an example, through the identity authentication during the wizard installation process for platform collaboration enterprise and the verification of integrity and confidentiality during the process of registration service information, the usability and effectiveness of the proposed method was proved.

Key words: industrial chains; software as a service; multi-source; dynamic integration; data security; encryption technology

0　引言

当前,企业的信息化程度越来越高,对信息管理的需求也越来越复杂,为此人们开发和应用了大量的应用系统和业务系统来提高工作效率和服务水平,然而也导致系统间信息资源的集成越来越难,很难将各系统数据资源信息共享和整合。软件即服务(Software a Service, SaaS)充分利用网络技术与资源共享的特性,成为信息集成产业的主流[1],很好地解决了异构信息系统间数据的交换和共享,其更加开放的系统环境和网络结构,加重了系统在各个环节和领域所面临的安全威胁,使其成为 SaaS 平台信

收稿日期:2014-06-09;**修订日期**:2014-09-24。Received 09 June 2014; accepted 24 Sep. 2014.
基金项目:国家 863 计划资助项目(2013AA040606)。**Foundation item**: Project supported by the National High-Tech. R&D Program Fundation Projects, China (No. 2013AA040606).

息集成亟待解决的问题。文献[2]主要研究了数据完整性、传输保密性、业务协作不可抵赖性等数据安全问题。文献[3-4]主要研究了服务集成安全的加密技术及认证方法等。文献[5]研究了产业链协同 SaaS 平台流程定制中的安全问题，提出了一种流程定制的安全控制模型。文献[6]研究了 SaaS 平台中的用户数据安全问题，利用平台提供数据库接口，通过第三方数据库服务保证用户数据安全。

本文在上述研究的基础上，针对产业链协同 SaaS 平台[7]上多源信息动态集成中存在的安全隐患，利用数据加密技术[8-9]、Hash 技术、数字签名技术[10-12]和 Web Service[13]技术等，提出了面向产业链协同 SaaS 平台的多源信息动态集成安全解决方案。

1 产业链协同 SaaS 平台多源信息动态集成安全需求

1.1 产业链协同 SaaS 平台多源信息动态集成方案

面向产业链协同 SaaS 平台的多源信息动态集成主要是为屏蔽各企业在平台数据结构和语义等的异构，实现数据的无缝集成，在现有平台模型和架构[14]的基础上，通过建立平台私有统一描述、发现和集成协议(Universal Description, Discovery and Integration, UDDI)中心，将多源信息数据格式转换设计为集成向导，安装在各个协作企业内部，通过 Web Service 向平台的 UDDI 中心的注册服务和查询服务操作，满足平台盟主企业对不同协作企业不同数据源动态调用的需求，其内容主要包括协作企业客户端多源信息集成模块、协作企业向平台 UDDI 中心的注册模块以及盟主企业通过平台查询注册的服务模块，以产业链协同平台上经销商的车辆社会库存信息为例，其具体过程如图 1 所示。

1.2 产业链协同 SaaS 平台多源信息动态集成安全需求

由图 1 所示的多源信息动态集成过程可以看出，其整个过程主要包括下载集成向导→信息格式转换→注册服务→查询服务，在以上四个环节中，若集成向导被非法下载安装，则服务信息被非法修改、注册、访问都将给平台带来一定的安全隐患，具体表现如下：

(1)集成向导下载安装的安全需求

集成向导是平台提供给授权合法用户的工具，为保证平台和联盟企业的利益，应保证平台用户能安全下载集成向导并顺利安装，非授权用户可以下

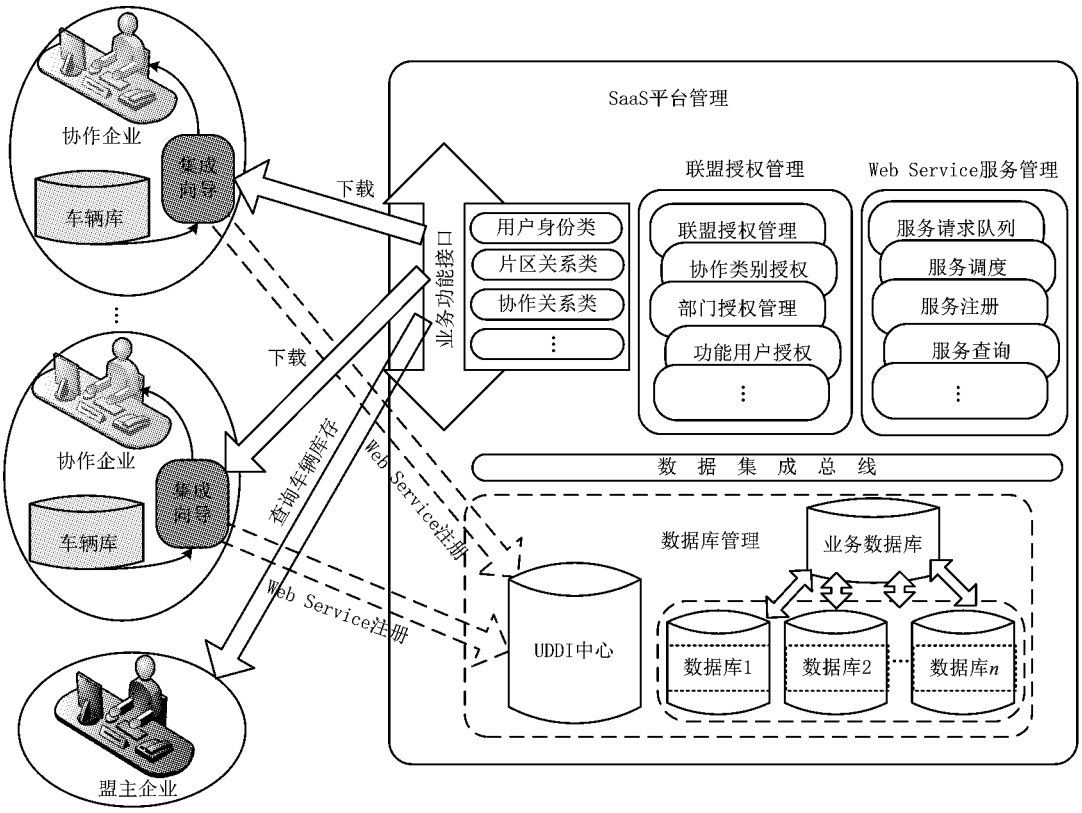

图1 面向SaaS平台多源信息动态集成方案

载,但无法通过向导发布服务信息。

(2)集成向导注册 Web Service 信息的安全需求[15]

保证发布的服务不是虚假的服务和恶意服务,对协作企业注册服务时的注册请求进行身份验证和权限验证,保证客户端到平台数据中心服务请求的安全,确保注册到平台 UDDI 中心的服务信息没有经过非法修改。以整车库存信息为例,平台 UDDI 服务中心没有授权协作企业 A 发布整车库存信息服务。一旦协作企业 A 发布整车库存信息服务,就会变成虚假服务和垃圾服务而影响平台性能,而且如果中间被非法篡改为配件库存信息注册到平台 UDDI 中心,将直接导致查询结果出错。

(3)基于片区调用 Web Service 时的安全需求

协作企业注册 Web 服务到平台,保证注册信息的安全,防止服务使用者——盟主企业的敏感、私人的机密数据被非法截取。为了更好地对注册的 Web Service 进行管理,本文采用基于片区的方式来调用所注册的服务,盟主企业调用注册服务时,只能调用本联盟片区内的服务,以需求(2)为例,协作企业 A 所属的盟主企业不能调用其他联盟片区内协作企业所注册的服务。

2　产业链协同 SaaS 平台多源信息动态集成安全模型

2.1　SaaS 平台多源信息动态集成安全控制模型

为实现对 SaaS 平台上多源信息动态集成过程安全的控制,根据以上安全需求分析,建立了面向 SaaS 平台多源信息动态集成安全模型,对集成安全模型中涉及的相关对象进行如下定义:

定义 1　产业链协同 SaaS 平台多源信息集成安全模型应用对象中,企业联盟 U_i 可用一个四元组 $U_i=(E_{U_i},T_{U_i},R(T_{U_i}),E\rightarrow R(T_{U_i}))$表示。其中:

$E_{U_i}=\{E_1,E_2,\cdots,E_m\}$表示联盟中的企业,$m$ 为企业数量;

$T_{U_i}=\{T_{U_i1},T_{U_i2},\cdots,T_{U_in}\}$表示联盟企业协作关系类型集,包括经销商、服务商、供应商等协作关系类别;

$R(T_{U_i})$表示按协作关系类型对企业划分的片区级,则对任意片区 A_i 有 $T_{U_i}\rightarrow A_i$ 的映射关系。盟主企业可以对每个协作类别设置划分片区,建立协作类别与片区的关系;

$E\rightarrow R(T_{U_i})$表示联盟 U_i 中的协作关系集。

盟主企业对应的管理岗位可对该协作类别企业的操作员进行管理,盟主企业可按协作类别创建业务员,盟主企业可按协作类别的片区为其指定业务员,一旦指定片区关系,业务员将具有操作该片区对应的业务功能。

定义 2　产业链协同 SaaS 平台多源信息集成安全模型应用对象中,联盟业务员管理 $ROLE_j$ 可用一个三元组 $ROLE_j=(E_{ROLE_j},C_{ROLE_j},E\rightarrow R(ROLE_j))$表示。其中:

$E_{ROLE_j}=\{E_1,E_2,\cdots,E_n\}$表示盟主企业角色,盟主企业可以按协作类别创建业务员,n 表示业务员数量;

$C_{ROLE_j}=\{C_1,C_2,\cdots,C_m\}$表示协作企业角色,盟主企业对应的管理岗位可对该协作类别企业的操作员进行管理;

$E\rightarrow R(ROLE_j)$表示业务员片区管理协作关系。

安全模型主要涉及用户身份认证安全、注册服务信息安全、注册服务信息完整性验证安全三个方面,其中协作企业 C_{ROLE_j} 在平台上下载集成向导后,为保证其为平台授权的合法用户角色,需要进行身份认证,身份认证的模式可用如下形式描述:

$$Authent=(MI_l,DM_l,UserInf_l,Serv_l,O_l)。\quad(1)$$

其中:

MI_l 表示协作企业 C_{ROLE_j} 下载的多源信息集成向导;

DM_l 表示安装用户加密信息所用的算法,由安装向导的协作企业 C_{ROLE_j} 提供;

$UserInf_l$ 表示用户登录验证信息,且 $UserInf_l=(User_{lName},User_{lPassword})$,表示用户登录的用户名和密码;

$Serv_l$ 表示协作企业需要注册的服务信息,且 $Serv_l=(Serv_{lnm},Serv_{lad})$,表示注册服务的名称和服务的地址;

O_l 表示集成向导 MI_l 注册服务 $Serv_l$ 的所属业务。

为保证式(1)中注册服务信息的安全性及注册信息完整性的验证,对其涉及的对象定义如下:

定义 3　多源信息集成向导得到的平台通过加密算法 DM 计算得到的用户信息摘要用 $Abstract_i$ 表示,本地用户信息通过加密算法 DM 进行加密后的内容用 $A\_encrypted_i$ 表示。

由式(1)和定义 3 可知:

$$A\_encrypted_i=DM(UserInf_l)。\quad(2)$$

如果 $A\_encrypted_i = Abstract_i$，则验证登陆信息合法。

为保证注册、调用 Web Service 过程中数据的完整性和保密性，其验证过程可以用以下表达式表示：

$$VER = (UserInf_l, Infor_m, E_m, T_m)。 \quad (3)$$

其中：

$UserInf_l$ 表示用户信息(如式(1))；

$Infor_m$ 表示用户要注册的信息，且 $Infor_m = (Corp_m, Serv_m)$，其中：$Corp_m$ 表示注册企业名称，$Serv_m$ 表示注册的服务信息；

E_m 表示盟主企业加解密，其中盟主企业公私密钥对用 (KU_E, KR_E) 表示，负责对注册信息的加密，保证传输数据不能被非法截获；

T_m 表示协作企业加解密，其中协作企业公私密钥对用 (KU_T, KR_T) 表示，用私钥对注册信息进行加密，将密文利用 Hash 函数生成摘要，保证传输数据的完整性。

定义 4 用 $V\_Abstract$ 表示 Hash 函数对协作企业私钥 KR_T 加密的注册密文 $KR_T(A\_encrypted_i)$ 生成的摘要，$D\_Abstract$ 表示盟主企业利用协作企业公钥 KU_T 解密生成的密文 $KU_T(A\_encrypted_i)$ 用相同的 Hash 函数生成的摘要。

由式(2)、式(3)和定义 4 知：

$$V\_Abstract = Hash(KR_T(A\_encrypted_i))；(4)$$

$$D\_Abstract = Hash(KU_T(A\_encrypted_i))。(5)$$

由以上可得，协作企业注册信息的验证过程为：$(A\_encrypted_i = Abstract_i) \cap (V\_Abstract = D\_Abstract) = true$，注册信息真实可靠，可进行注册或查询。

2.2 基于身份及业务驱动的安全模型执行策略

为保证只有与业务相关及身份认证的合法对象才能访问和执行安全模型，多源信息集成安全模型采用基于身份及业务驱动的模型执行策略，实现产业链协同平台对不同联盟企业信息集成安全的需求。

基于身份及业务驱动的模型执行策略所涉及的对象由一个二元组 $HP = (O_l, UserMess_l)$ 表示。其中：

O_l 表示注册服务所属的业务(如式(1))；

$UserMess_l$ 表示执行业务活动的用户信息，$UserMess_l = (E_{U_l}, R(T_{U_l}), Privilege_l)$，由定义 1 知，$E_{U_l}$ 表示用户所属的联盟企业，$R(T_{U_l})$ 表示按协作关系类别对应企业用户划分的片区，$Privilege_l$ 表示用户执行业务活动的权限。

集成向导注册服务所属的任意业务 O_l，其具体的驱动模型算法如下。

算法 1 安全模型驱动算法。

输入：用户 P 信息 $UserMess_l$，业务名称 O_l；

输出：模型执行结果。

步骤 1 验证用户 P 的信息 $UserMess_l$，判断是否为平台合法用户，如果是则转步骤 2，否则退出。

步骤 2 由所属片区 $R(T_{U_l})$，得到 P 对应的盟主企业角色 E_{ROLE_j} 或协作企业角色 C_{ROLE_j}。

步骤 3 VER 验证注册信息，如果 $(A\_encrypted_i = Abstract_i) \cap (V\_Abstract = D\_Abstract) = true$，则可进行注册和查询服务，则转步骤 4。

步骤 4 根据用户角色，如果是 C_{ROLE_j}，则根据对应的权限 $Privilege_l$，执行注册服务业务 O_l；如果是 E_{ROLE_j}，则根据对应的权限 $Privilege_l$，执行查询服务业务 O_l。

步骤 5 算法结束。

3 产业链协同 SaaS 平台多源信息动态集成安全解决方案

3.1 SaaS 平台多源信息动态集成安全解决方案的实现

根据面向产业链协同 SaaS 平台多源信息动态集成对数据安全的要求，设计了如图 2 所示的信息集成安全解决方案。本解决方案主要包括：①平台协作企业下载集成向导安装的身份验证；②协作企业注册服务信息过程中数据的完整性验证；③平台盟主企业查询平台信息过程中数据的保密性验证。

以上解决方案主要涉及以下 2 个主要功能模块：

(1)平台客户端模块

平台客户端包括协作企业和盟主企业两类用户，协作企业用户主要负责下载安装集成向导，通过用户信息加密及使用 U 盾验证用户为合法用户，注册需要的服务信息；盟主企业用户主要负责在客户端解密注册信息密文，查看协作企业注册的服务信息。

(2)平台服务端模块

平台服务端主要包括存储集成向导，对注册信息利用 Hash 函数生成摘要，负责注册信息完整性的验证，防止注册信息被非法截获，保障盟主企业用

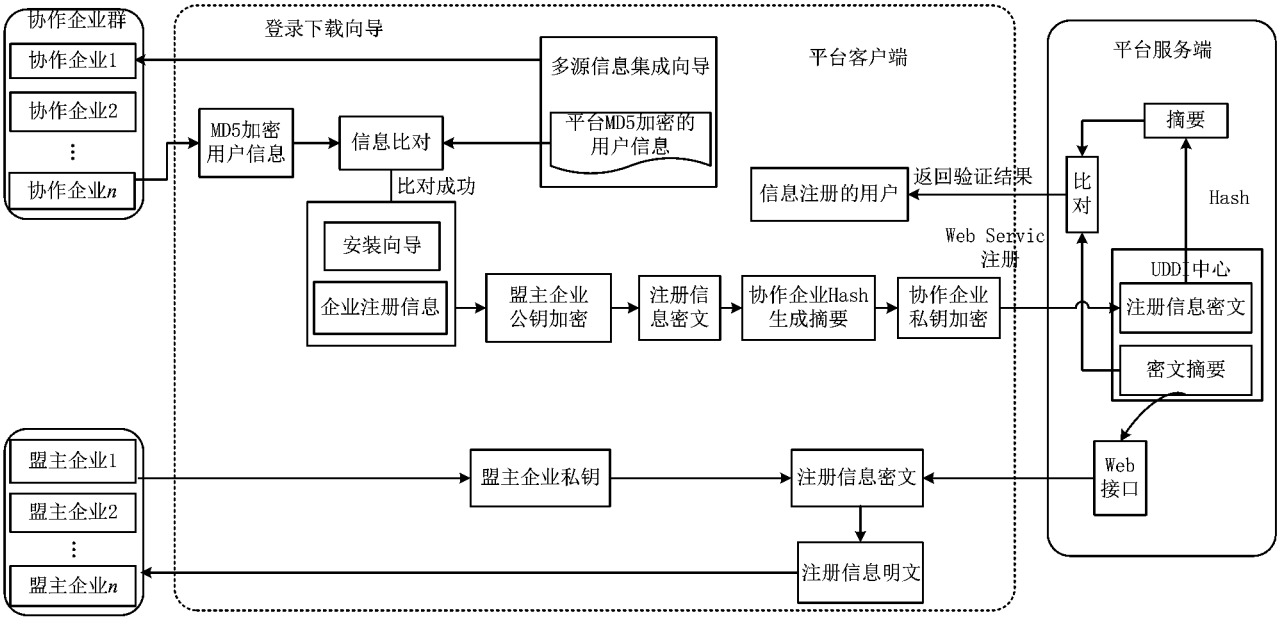

图2　面向SaaS平台多源信息动态集成安全解决方案

户的正确调用服务等。

3.2　基于身份认证和加密技术的集成安全策略

本文通过基于身份认证机制,将用户划分为应用程序定义的逻辑角色,使用访问控制技术和数据加密传输机制实现用户的透明实效访问,具体如下。

(1)基于平台用户信息的身份认证

Hash 函数 MD5 不依赖任何密码系统和假设条件,是一种常用的简单高效的加密算法。产业链协同平台用户信息的加密采用 MD5 加密,将平台的用户信息先打包在向导中,供企业一起下载,具体的认证流程如图 3 所示,实现的身份认证算法如下:

算法 2　用户信息的身份认证算法。

步骤 1　协作企业用户 C_{ROLE_j} 登录平台,下载多源信息集成向导 MI_l。

步骤 2　C_{ROLE_j} 根据用户的身份信息 $UserInf_l$,由协作关系 T_{U_i} 获得下载加密信息权限。

步骤 3　由步骤 2 中的权限获得向导中对应的平台 MD5 加密的用户信息摘要 $Abstract_i$。

步骤 4　用户安装集成向导,利用 MD5 加密自己的用户信息 $UserInf_l=(User_{lName},User_{lPassword})$,获得摘要 $A\_encrypted_i$。

步骤 5　使用 U 盾验证用户身份信息并比对步骤 4 和步骤 5 中的摘要,如果 $A\_encrypted_i=Abstract_i$ 则可顺利安装,否则提示退出。

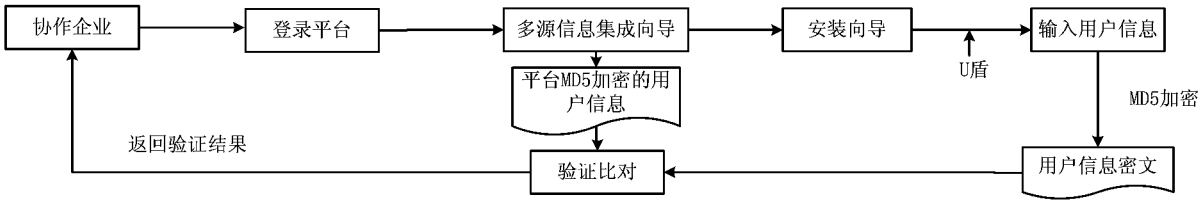

图3　身份认证流程

(2)基于非对称加密的数据保密性

在协作企业注册服务信息的过程中,为保证注册信息不被非法截获,保障用户信息的安全性,协作企业只负责信息的注册而不通过平台查看,因此本文通过基于盟主企业公钥加密的方式来保证数据的保密性,具体流程如图 4 所示,实现的加解密算法如下:

算法 3　数据加解密算法。

步骤 1　协作企业用户 C_{ROLE_j} 利用对应盟主企业的公钥 KU_E 加密需要注册的信息 $Infor_m=(Corp_m,Serv_m)$,生成密文。

步骤 2　将步骤 1 中的密文注册到平台。

步骤 3　盟主企业 E_{ROLE_j} 登录平台,利用自己的私钥 KR_E 解密步骤 1 中的密文,得到明文。

(3)基于 Hash 算法的数据完整性验证

本文通过基于 Hash 算法的方式来保证数据在传输过程中的完整性,首先将以上协作企业注册的信

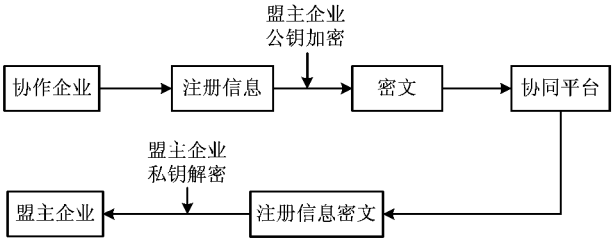

图4 数据加解密流程

息密文生成摘要。为了保证 Hash 生成摘要的安全，利用协作企业的私钥对生成的摘要进行加密，具体流程如图 5 所示，实现的数据完整性验证算法如下。

算法 4 数据完整性验证算法。

步骤 1 协作企业用户 C_{ROLE_j} 利用 Hash 算法将注册信息 $Infor_m=(Corp_m, Serv_m)$ 密文生成摘要。

步骤 2 C_{ROLE_j} 利用自己的私钥 KR_T 对步骤 1 中的摘要进行加密，生成密文。

步骤 3 将步骤 2 中的密文注册到平台。

步骤 4 平台利用协作企业的公钥 KU_T 解密步骤 2 中的密文。

步骤 5 对步骤 3 中解密的密文，利用步骤 1 中的 Hash 算法生成摘要。

步骤 6 比对步骤 1 和步骤 5 中的摘要，如果相同则数据是完整的，否则提示数据被篡改。

具体流程如图 5 所示。

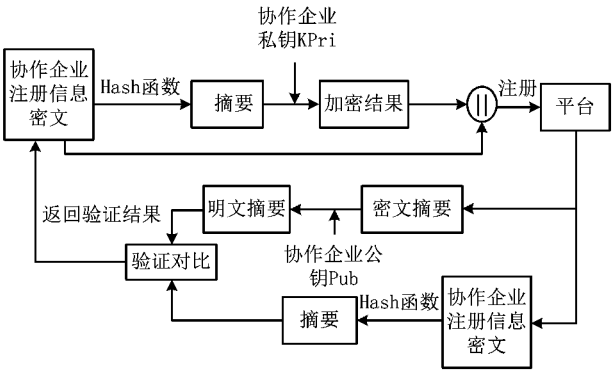

图5 数据完整性验证流程

协作企业注册 Web Service 到平台，盟主企业登录平台采用面向片区的服务动态调用方式，按片区分别调用注册的服务，实现的调用算法如下：

算法 5 面向片区的 Web 服务动态调用算法。

步骤 1 盟主企业 E_{ROLE_j} 登录平台。

步骤 2 平台根据用户身份信息 $UserInf_l$，得到对应片区 $R(T_{U_i})$ 的协作企业。

步骤 3 根据 C_{ROLE_j} 查找平台 UDDI 中相应的注册服务，提取该服务信息的密文。

步骤 4 利用盟主企业的私钥 KR_E 解密步骤 3 中的密文，得到注册信息明文 $Infor_m=(Corp_m, Serv_m)$。

步骤 5 获得平台标准数据结构的 xml 文件，按照标准数据结构生成空的数据集。

步骤 6 调用所属片区 $R(T_{U_i})$ 协作企业 C_{ROLE_j} 的 Web 服务，将查询结果存入步骤 5 生成的数据集中。

步骤 7 根据服务 WSDL 文件中的 Web 所支持的方法，动态调用 Web 的方法。

步骤 8 将步骤 7 中的结果存入数据集，返回调用结果。

4 应用验证及算法分析

4.1 应用验证

产业链协同 SaaS 平台采用浏览器/服务器(Browser/Service, B/S)结构，在 .Net 环境下开发实现，经销商社会库存是汽车产业重要的业务功能，以产业链协同平台协作企业的车辆库存信息为例，验证本文提出的解决方案可以满足平台多源信息动态集成安全的需求，具体分析如下。

(1)某平台协作企业集成向导安装验证

平台上协作企业的用户信息如表 1 所示，其中用户名、密码等敏感字段为 MD5 加密的，以可扩展标记语言(eXtensible Markup Language, XML)文档格式打包在集成向导中。企业用户通过浏览器访问平台可以下载集成向导，如果要安装则要求必须填写用户名和密码，点击“下一步”安装时，同时用 MD5 加密此安装信息、生成密文，具体如表 1 中的密文所示。将此密文与向导中已有的平台中加密的用户信息进行比对，如果信息不匹配则不是平台授权用户，无法安装集成向导，如图 6 所示。为保证用户的登录信息不被非法获取，在完成用户注册信息认证之后再对输入信息的用户进行 U 盾验证，如图 7 所示。

表 1 MD5 加密用户名和密码密文

UserName	Password	MD5 加密后的密文
xy	111111	96E79218965EB72c92A549DD5A330112
Lxl	Lxl110	41DDBBF0C23FE6C947C58F481C444C63
Hzx	19hz88	001D9577582459CBE7A8B1C3105B8sFB
Littlered	Lith. h	0FE3586A798E098B303E22F73DBD8882E

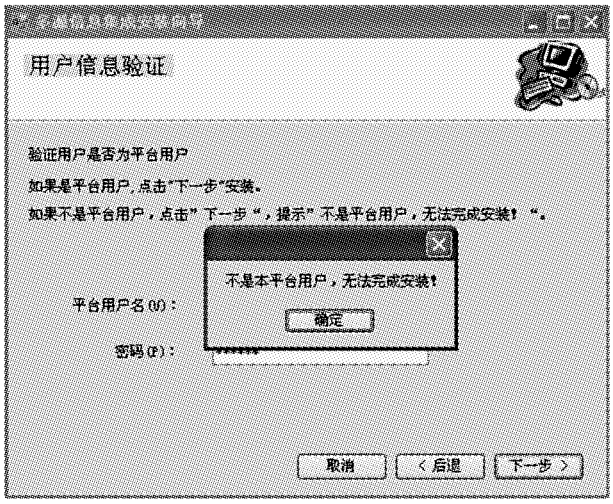

图6　用户注册信息身份认证界面

图7　U盾验证界面

(2)某平台协作企业注册 WS 信息安全验证

1)在集成向导安装过程中,非授权用户无法完成最后的注册且协作企业注册服务只能注册到平台对应的自己的 UDDI 中心,如果注册的服务与企业不对应,则给出提示信息,如图 8 所示。

2)如果平台 UDDI 中心已经存在服务,则协作企业不能重复注册此服务,只能修改。以平台某协作企业的车辆库存信息为例,其已在平台的 UDDI 服务中心注册了车辆库存查询信息,如图 9 所示。

此时企业安装集成向导、注册车辆库存查询服务时,会提示服务已经存在,不能重复注册,如图 10 所示。

(3)某平台盟主企业通过平台调用 WS 注册信息安全验证

盟主企业通过平台只能调用本联盟协作企业所

图8　注册服务身份认证界面

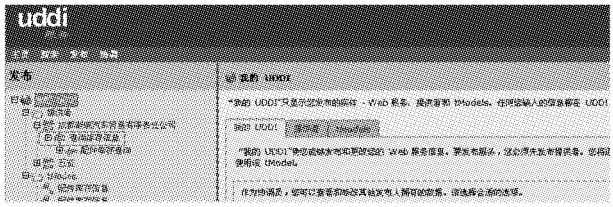

图9　UDDI中心已注册服务界面

图10　服务重复注册验证界面

注册的 Web 服务信息,无法查看其他联盟中所注册的服务,即使非法获取了其他注册信息,看到的也只是密文。协作企业注册到平台的信息主要包括服务名称和服务地址,基于. Net 框架中 AESHelper 类,利用 AES 对称加密算法对注册信息进行加密,以密文的形式存在平台 UDDI 中心,平台数据库中注册信息的对应密文信息如表 2 所示。

表 2 平台数据库注册信息对应密文

协作企业注册信息	平台存储的加密结果
四川片区	+3t8yM5wd/nXjaFlTciLdQ==
成都新瑞汽车贸易有限责任公司	+qYOI7Yq3WfZasPEVJIpzIdm/CIBVayUsF+m2sJiV6yk2OZNHPIzZ9GVXu6OpoA3
查询库存信息	Pb6FIVJGeyPQl7d7O4uXtjkkl6bScUgJCBn3fYCrKTFZgL7Tc4X+VL75ELdVEJbU
http://192.168.1.19/Exercise/Service1.asmx	TJsnH6o1eZL6LAnBnR3OkVDAqaVrNP8FslbzP3hClJgnsk4djyc7nb07oW8AXzZ1
XY	gw9jTdWNgzuBoNnoVgJHEQ==

4.2 算法安全性及性能分析

在上文具体应用验证的基础上，对方案中算法的安全性及性能分析如下：

(1)安全分析

1)存储安全性。方案中主要涉及客户的用户身份信息和注册服务信息，其中企业通过 MD5 加密自己的身份信息并通过 U 盾来防止信息被非法截获，保证了客户端用户信息的存储安全；服务信息通过盟主企业公钥加密，以密文的方式存储在平台 UDDI 中心(如表 2)，平台管理员及盟主企业非授权用户看到的都是密文，在很大程度上保证了服务信息的存储安全性。

2)传输安全性。注册信息通过盟主企业公钥加密，摘要信息利用注册企业私钥加密，传输过程中的数据信息都以密文的形式传输，传输的都是加密后的密文，保证了数据传输的保密性。

3)数据的完整性。平台利用 Hash 函数生成摘要并与企业注册服务信息摘要进行比对，具体流程如图 5 所示。

(2)性能分析

安全解决方案主要涉及 MD5 加密、对称加密、非对称加密等算法，根据现有平台的特点，对采用策略、算法的必要性进行了说明，验证了方案的优点和有效性、易用性，具体分析如下：

1)由于此认证是面向集成安装向导，针对注册用户基本信息的特点，从简单、易用性来考虑，采用基于用户身份信息的认证策略。

2)针对简单、单向加密的特点加密主要是注册信息的用户名、密码等敏感字段，采用 MD5 加密，并加入 U 盾来防止初始信息被非法截获，改善了其加密密码一成不变的缺点。

3)根据协作企业注册服务信息，以及对应的盟主企业查看的分布式系统特点，采用非对称加密方式，盟主企业公钥加密注册信息；在信息完整性验证过程中，考虑加密效率及需在平台服务端进行验证的特点，采用协作企业对称密码加密摘要的方式。

协作企业从注册安装向导到盟主企业通过平台获取库存信息的整个过程中，经过多次加解密算法较好地适应了当前平台的需求，具体性能分析如表 3 所示。客户端 MD5 加密算法主要针对用户名、密码等敏感字段；非对称加密针对服务名称、服务地址等敏感字段；对称加密只针对 Hash 函数生成的摘要，加密量很小，需要的平均时间小于 10 ms。盟主企业进行远程解密查看计算需要的平均时间小于 250 ms(测试计算机均为 PC 机，CPU 内存 2 G)，因此算法是可行的。

表 3 算法性能分析

算法名称	客户端加解密操作	服务端加解密操作
用户信息的身份认证算法	MD5 加密 1 次	无
数据加解密算法	盟主企业公钥加密 1 次、盟主企业私钥解密 1 次	无
数据完整性验证算法	注册企业私钥加密 1 次	注册企业公钥解密 1 次

5 结束语

本文基于笔者前期所做的产业链协同 SaaS 多源信息动态集成，针对协作企业与平台信息集成安全的需求，通过平台协作企业向导安装过程中身份验证、注册信息的加解密完成服务的注册和查询，平台服务端实现注册信息的完整性验证等，基本满足了现有平台动态集成安全的需求。

本文只是探讨性地提出了一种解决方案，下一步的研究方向有：①身份认证方面，可以借鉴当前的最近研究进展，使用更安全高效的验证策略。②注册服务方面，可进一步从 Web Service 协议等服务本身的安全考虑。③集成安全方面，应该对现有加解密算法进行优化，以提高算法效率。

参考文献:

[1] ZHOU Liang, CAO Jian, CHEN Jiaojuan. Self-envolving for process model of software as a service[J]. Computer Integrated Manufacturing Systems, 2011, 17(8): 1603-1608(in Chinese).[周　亮,曹　健,陈姣娟.软件即服务流程模型的自动演化[J].计算机集成制造系统,2011,17(8):1603-1608.]

[2] CHEN Jing, SUN Linfu. Solutions of data security for industrial chain collaboration public service platform based on SaaS [J]. Computer Integrated Manufacturing Systems, 2011, 17(6):317-324(in Chinese).[陈　静,孙林夫.基于 SaaS 的产业链协作公共服务平台数据安全解决方案[J].计算机集成制造系统,2011,17(6):317-324.]

[3] YU Yonghong, BAI Wenyang. Integrated security over outsourced database services based on encryption[J]. Journal of Computer Applications,2011,31(1):110-115(in Chinese).[余永红,柏文阳.基于加密技术的外包数据库服务集成安全[J].计算机应用,2011,31(1):110-115.]

[4] CHEN Jing, SUN Linfu. One-time password authentication based on double random soft input model[J]. Journal of Sichuan University: Engineering Science Edition, 2010, 42(2): 154-159(in Chinese).[陈　静,孙林夫.基于双随机软输入模型的一次性口令认证方法[J].四川大学学报:工程科学版,2010,42(2):154-159.]

[5] CAO Shuai, WANG Shuying. Research on security technology of workflow customization for collaborative SaaS platform of industrial chains[J]. Computer Science, 2104, 41(1): 230-234 (in Chinese).[曹　帅,王淑营.产业链协同 SaaS 平台业务流程定制安全技术研究[J].计算机科学,2104,41(1):230-234.]

[6] ZHANG Qiang, CUI Dong. Enhance the user data privacy for SAAS by separation of data[C]//Proceedings of 2009 International Conference on Information Management, Innovation Management and Industrial Engineering. Washington, D. C., USA: IEEE Computer Society, 2009: 130-132.

[7] PAN Hua, SUN Linfu, LIU Shuya. Research on the personality customizable dynamic form technology for SaaS platform [J]. Application Research of Computers, 2013, 30(10): 3026-3029(in Chinese).[潘　华,孙林夫,刘述雅.面向 SaaS 平台的动态表单定制技术研究[J].计算机应用研究,2013,30(10):3026-3029.]

[8] WANG Dakang, DU Haishan. Encrypt&crack technology in information security[J]. Journal of Beijing University of Technology, 2006, 32(6): 497-500(in Chinese).[王大康,杜海山.信息安全中的加密与解密技术[J].北京工业大学学报,2006,32(6):497-500.]

[9] YUAN Chun, WEN Zhenkun, ZHANG Jihong, et al. Progress of cryptographic access control and encryption security database[J]. Acta Electronica Sinica, 2006, 34(11): 2043-2046 (in Chinese).[袁　春,文振堃,张基红,等.基于密码学的访问控制和加密安全数据库[J].电子学报,2006,34(11):2043-2046.]

[10] XIANG Can, YOU Lin. A new conic curve digital signaturesScheme[C]//Proceedings of the 5th International Conference on Information Assurance and Security. Washington, D. C., USA: IEEE, 2009: 623-626.

[11] ZHANG Qiuxia, LI Zhan, SONG Chao. The Improvement of digital signature algorithm Based on elliptic curve cryptography[C]//Proceedings of the 2nd International Conference on Artificial Intelligence, Management Science and Electronic Commerce (AIMSEC). Washington, D. C., USA: IEEE, 2011: 1689-1691.

[12] JUNAID G, AIJAZ A M. Using digital signature standard algorithm to incorporate non-invertibility in private digital watermarking techniques[C]//Proceedings of the 10th ACIS International Conference on Software Engineering, Artificial Intelligences, Networking and Parallel/Distributed Computing. Washington, D. C., USA: IEEE, 2009: 399-404.

[13] YUE Kun, WANG Xiaoling, ZHOU Aoying. Underlying techniques for Web services: a survey[J]. Journal of Software, 2004, 15(3): 428-442(in Chinese).[岳　昆,王晓玲,周傲英.Web 服务核心支撑技术:研究综述[J].软件学报,2004,15(3):428-442.]

[14] CHEN Jing, WANG Shuying, SUN Linfu. Flexible model and architecture of public service platform for business related mult-industrial chain collaboration[J]. Computer Integrated Manufacturing Systems, 2011, 17(1): 177-185(in Chinese).[陈　静,王淑营,孙林夫.面向柔性的业务关联的多产业链协作公共服务平台模型和架构[J].计算机集成制造系统,2011,17(1):177-185.]

[15] GUTIERREZ C, FERNANDEZ-MEDINA E, PIATTINI M. PWSSec: process for Web services security[C]//Proceedings of IEEE International Conference on Web Services. Washington, D. C., USA: IEEE, 2006: 213-222.

作者简介:

潘　华(1982—),男,山东潍坊人,博士研究生,研究方向:产业链协同平台技术、商务智能等,E-mail:linqupanhua@126.com;

王淑营(1974—),女,天津人,研究员,博士,研究方向:网络化制造、电子商务公共服务平台;

孙林夫(1963—),男,浙江绍兴人,教授,博士生导师,研究方向:网络化制造技术、产业链协同技术及公共服务平台技术等;

吕　瑞(1988—),女,河南焦作人,博士研究生,研究方向:产业链协同平台技术、商务智能。