面向数据跨域流转的延伸访问控制机制

谢绒娜[1]，郭云川[2]，李凤华[1,2,3]，史国振[4]，王亚琼[1]，耿魁[2]

（1. 西安电子科技大学网络与信息安全学院，陕西 西安 710071；
2. 中国科学院信息工程研究所，北京 100093；
3. 中国科学院大学网络空间安全学院，北京 100049；4. 北京电子科技学院电子与通信工程系，北京 100070）

摘 要：针对复杂网络环境中数据跨域流转后的受控共享，提出了一种延伸访问控制机制。所提控制机制分为约束控制和传播控制 2 类，其中，约束控制解决访问请求实体在访问请求前对数据的访问授权问题，传播控制用于数据脱离数据中心后对数据的延伸控制。所提机制基于数据自身及数据流转过程中的起源信息，实现了对数据的直接和间接访问控制。理论分析证明了所提机制的安全性和有效性。以电子发票全生命控制为例，展示了所提机制的实施方法，该实例表明，所提机制能解决跨域跨系统交换后的数据细粒度延伸控制问题。

关键词：跨域；数据流控制；数据起源；延伸授权；传播控制

中图分类号：TP302

文献标识码：A

doi: 10.11959/j.issn.1000−436x.2019151

Extended access control mechanism for cross-domain data exchange

XIE Rongna[1], GUO Yunchuan[2], LI Fenghua[1,2,3], SHI Guozhen[4], WANG Yaqiong[1], GENG Kui[2]

1. School of Cyber Engineering, Xidian University, Xi'an 710071, China
2.Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China
3. School of Cyber Security, University of Chinese Academy of Sciences, Beijing 100049, China
4. Department of Electronics and Communication Engineering, Beijing Electronic Science and Technology Institute, Beijing 100070, China

Abstract: Aiming at the controlled sharing for cross-domain data exchange for complicated application systems, an extended access control mechanism was proposed. The control process was divided into two steps: constraint control and propagation control. The constraint control was used to ensure that access to data was authorized before access request, and the propagation control was used for further extension control after obtaining data access right. In addition, by considering data self and data provenance, the direct and indirect access control were realized. Theoretically, the security and effectiveness of the proposed mechanism were proved. Finally, taking the control of electronic invoice as an example, the implementation approach was proposed. The example shows that the proposed mechanism can perform the fine-grained extended control before and after data in the cross-domain and cross-system are exchanged.

Key words: cross-domain, data flow control, data provenance, extended authorization, propagation control

---

收稿日期：2018−11−06；**修回日期**：2019−03−24

通信作者：李凤华，lifenghua@iie.ac.cn

基金项目：国家重点研发计划基金资助项目（No. 2016YFB0801002）；国家自然科学基金资助项目（No.U1836203）；中国科学院战略先导专项基金资助项目（No.XDC02040400）

Foundation Items: The National Key Research and Development Program of China (No. 2016YFB0801002), The National Natural Science Foundation of China (No.U1836203), The Strategic Priority Research Program of the Chinese Academy of Sciences (No.XDC02040400)

1 引言

复杂网络环境中，运行着各种各样的大型应用系统，如专用系统、应急指挥系统、电子政务系统、电子商务系统等。这些大型应用系统为完成某项任务，往往需要多个子系统协同运作。比如专用系统中，一个简单的业务处理可能会涉及认证系统、业务系统、监管系统等子系统。数据需要在认证系统、业务系统、监管系统之间相互流转和共享。这些子系统大部分属于不同管理域，部署在不同地域。数据跨系统跨域流转已成为复杂网络环境数据共享的趋势，如何确保数据跨系统跨域流转后的受控共享是访问控制面临的重大挑战。

复杂网络环境下，数据在不同实体、不同系统、不同域之间流动形成了数据流。数据跨系统、跨域流转中的延伸访问控制是数据流转和共享过程中急需解决的问题。以专用系统为例，当数据在同一个子系统中的不同实体之间流转，或者从一个子系统流转到另一个子系统、一个域流转到另一个域时形成了数据流。在数据流转过程中，数据所有者一旦将数据发送给其他实体，就失去了对数据的控制。数据接收者在得到数据后，可以对数据进行任意修改和转发。

数据或信息在不同系统、不同域之间的流动形成了数据流或信息流。针对数据流或信息流的访问控制，早期的文献[1-4]大多是针对软件程序、操作系统或应用系统中信息流的控制。Bell 等[5]和 Biba 等[6]分别提出的 BLP（Bell and LaPadula）和 Biba 访问控制模型解决了多级安全系统中信息流机密性和完整性问题。Zeldovich 等[7]将信息流控制从单个系统引入网络环境中，实现了多个不可信服务系统之间的信息流控制。She 等[8]将基于角色的访问控制与起源数据相结合，利用起源数据对数据可信度进行评估，根据信任值评估结果对信息流进行访问控制。为提高信息流转的效率，She 等[9]提出服务组合协议，通过在信息流转前服务组合阶段对候选的服务器进行评估和访问控制策略的验证，改善了由于服务失效导致信息流转效率降低的问题。上述模型没有解决数据流转过程中的延伸控制问题。Asuquo 等[10]为了解决时延/中断容忍网络（DTN, delay/disruption tolerant network）在数据转发过程中的访问控制问题，提出了分布式信任管理模型评估中间节点的可信性，从而实现了对数据转发的访问控制。Li 等[11]提出了强制性基于内容访问控制机制，实现了数据中心网络数据流转过程中间节点对数据缓存权限的控制。上述文献只是针对特殊应用场景，没有对延伸控制操作进行细粒度延伸控制。

数据在全生命周期流转过程中，来源于不同域、不同系统中的不同实体对数据各部分进行不同的操作，最终生成数据和数据流。数据跨系统、跨域流转过程中共享延伸授权的访问控制面临如下挑战。

1) 延伸授权的访问控制

对数据跨域流转的访问控制，不仅需要在访问请求前判断访问请求实体是否有访问的权限，还需要考虑访问请求实体得到访问权限后对数据资源进一步的延伸控制问题。对数据进行共享延伸的访问控制，访问请求实体不仅要考虑对数据本身的访问权限，还需要考虑对数据在整个流转过程中起源数据的访问权限。

2) 跨域流转的隐私泄露

为了实现跨域访问控制，很多文献采用基于角色或基于属性的访问控制机制。当数据在 2 个不同域之间流转时，不同域之间需要进行角色或属性的映射，这样势必会存在映射关系复杂、映射表维护成本高和隐私泄露的问题。如何降低数据跨域流转中隐私泄露问题是数据跨域流转延伸访问控制中急需解决的问题。

针对上述问题，本文提出了面向数据跨域流转的延伸访问控制机制，主要贡献如下。

1) 提出了面向数据跨域流转的延伸访问控制机制，并给出了形式化描述。该机制将访问控制分为约束访问控制和传播访问控制 2 类。其中，约束访问控制用于解决访问请求实体在访问请求前对数据资源的访问授权问题，传播访问控制用于解决访问请求实体得到数据资源访问授权后进一步的延伸控制问题。

2) 面向数据跨域流转的延伸访问控制机制基于访问请求实体和客体的属性进行访问授权，并把数据流转过程的起源数据作为客体的属性，实现访问请求实体对数据流的间接访问控制。在数据跨域流转时，不同域访问请求实体和客体通过属性映射，实现域内局部属性与全局属性的映射，进而实现不同域之间属性映射，避免了不同域之间直接进行属性映射造成的属性映射维护成本高、扩展性差的问题，同时降低了不同域之间属性映射导致的隐

私泄露的风险。

3) 对面向数据跨域流转的延伸访问控制机制的安全性和有效性进行了分析，并通过电子发票全生命周期的流转过程展示了数据跨域流转的延伸访问控制机制实施方法。安全性和性能分析表明，该机制有效解决了数据跨域随机流转过程中的延伸授权问题，并在保证安全性的前提下，有效提高了访问控制的效率。

2　相关工作

数据或信息在不同系统、不同域之间的流动形成了数据流或信息流，其中，信息代表有一定意义的数据。关于数据流或信息流访问控制，早期的文献大多集中在信息流访问控制。对于信息流的访问控制，部分文献采用起源数据进行访问授权。本节从信息流访问控制和基于起源的访问控制 2 个方面讨论数据跨域流转访问的研究进展。

2.1　信息流访问控制

对于信息流控制，早期的文献[1-4]大多是针对软件程序、操作系统或应用系统中信息流的控制，保证敏感信息不能输出到公共端口，并且关键的计算组件不能受到外部信息的影响。BLP 访问控制模型[5]将主体和客体分成不同的安全等级，通过“下读上写”的安全策略解决了多级安全系统中信息流机密性。参考 BLP 模型，Biba 访问控制模型[6]将主体和客体赋予不同完整性标记属性，通过“上读下写”安全策略实现了多级安全系统的完整性。Zeldovich 等[7]将信息流访问控制从单个系统引入网络环境中，实现了多个不可信服务系统之间的信息流控制。Groef 等[12]设计开发了一个 Web 浏览器，通过浏览器实现灵活准确的信息流控制。但上述文献大多是在执行过程的访问控制，对于信息流动前不同服务器组合时期的访问控制问题很少考虑，影响了信息流访问控制执行的效率。针对上述问题，She 等[9,13-14]提出了服务组合协议，将服务组合分成 3 个阶段进行服务器评估和访问控制策略的验证，从而实现了可信服务器组合，提高了访问控制的效率；同时，引入了转移因子（TF, transformation factor）的概念，提高了中间服务器访问控制执行的效率。但其没有考虑信息流转过程中的延伸控制。针对特殊应用场景下信息流的访问控制问题，近期不少文献提出了针对性的解决方案。为了解决时延容忍网络数据转发过程的访问控制问题。Asuquo 等[10]提出分布式信任管理模型，通过直接信任评估和间接信任评估相结合的方式实现对数据转发节点的可信性进行动态评估，从而实现对数据转发的访问控制，但只是针对 DTN 特殊网络环境，同样没有考虑数据流转过程延伸访问控制问题。Li 等[11]针对数据中心网络中的安全和隐私问题，提出了强制性基于内容的访问控制机制，内容提供者根据不同内容定义不同的安全标签，实现数据发送时中间节点对发送内容进行缓存的权限控制，虽然考虑了部分延伸控制问题，但只是针对数据中心网络这种特殊应用场景，中间节点对数据缓存及其他延伸操作没有进行进一步的细粒度控制。

2.2　基于起源的访问控制

起源数据主要用来跟踪、记录数据的生成过程，即记录谁在什么条件下对数据进行了什么操作。目前，不少文献利用起源数据进行数据流的访问控制。Park 等[15]提出了基于起源的访问控制模型，利用起源数据实现访问控制。为提高访问控制策略描述和执行的效率，Sun 等[16-17]设计了类型化的起源模型及其解释器，将起源数据当做一种特殊的属性进行访问控制。She 等[8]针对服务导向架构（SOA, service-oriented architecture）中的数据流跨域流转中的安全性和可信性问题，将基于角色的访问控制与起源数据相结合，根据起源数据对数据进行可信性评估，并根据信任值评估结果对数据流进行访问控制，通过域间角色的映射实现数据流跨域的访问控制，但存在映射表维护复杂以及域间角色映射造成的隐私泄露问题。李凤华等[18]提出了资源传播链来记录数据在不同实体之间的流转过程，实现了数据受控二次/多次分发，在一定程度上解决了数据资源的延伸控制问题，但没有给出延伸控制形式化的定义。

上述文献对数据跨域流转共享延伸访问控制问题都没有解决。

3　数据流模型

3.1　数据跨域流转的系统模型

数据跨域流转的系统模型如图 1 所示，包括多个不同类型的域。不同域包括各种实体（E, entity）、客体（O, object）、数据容器（DC, data container）、安全授权管理服务（SA, security authority）。其中，实体包括使用者、软件、硬件，客体包括各种数据资源（data），数据容器可以为文件夹、数据库、硬

盘等，安全授权管理服务负责访问控制策略管理、不同域间属性映射、访问控制判定和授权。

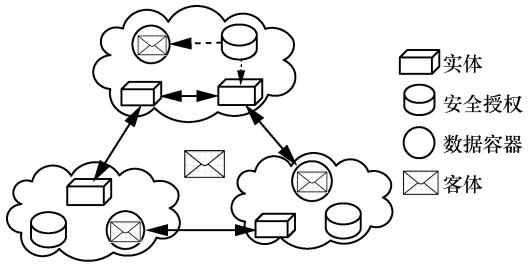

图 1 数据跨域流转系统模型

定义 1 数据跨域流转的系统包括域集合 $D=\{D_i|i\in N^*\}$，其中，N^* 为自然数集合。一个域 D_i 为四元组 $<D_i.E,D_i.O,\ D_i.\mathrm{DC},D_i.\mathrm{sa}>$，其中，实体集合 $D_i.E=\{D_i.e_j\mid j\in N^*\}$；客体集合 $D_i.O=\{D_i.o_j\mid j\in N^*\}$；数据容器集合 $D_i.\mathrm{DC}=\{D_i.\mathrm{dc}_j\mid j\in N^*\}$；$D_i.\mathrm{sa}$ 为域 D_i 的授权管理服务，管理域内和域间的访问控制策略集合 $D_i.\mathrm{Pol}=\{D_i.\mathrm{pol}_j\mid j\in N^*\}$。

3.2 数据流模型

不同实体、不同系统和不同域之间随机访问、生成和转发各种数据，形成了数据交互，如图 2 所示。

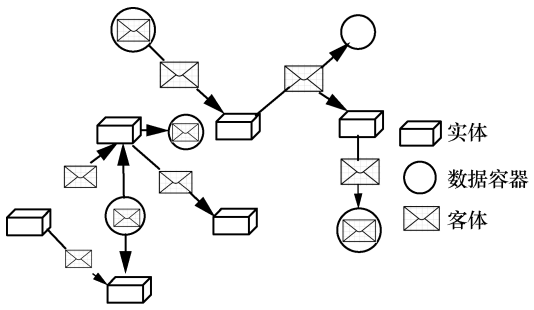

图 2 数据交互

域内的实体 e 接收其他实体发来的数据并作为自己的输入 $e.\mathrm{In}$，将输入的数据 $e.\mathrm{In}$ 和本地的数据 $e.L$ 通过函数 $e.F$ 生成输出数据 $e.\mathrm{Out}$，实体 e 对输出数据进行传播操作 $e.G$，发送给其他实体。数据流模型如图 3 所示。

定义 2 数据流模型 Q 为五元组 $<e.\mathrm{In},e.L,e.\mathrm{Out},\ e.F,e.G>$，其中，$e.\mathrm{In}$ 为输入数据的集合，$e.\mathrm{IN}=\{e.\mathrm{in}_k\mid k\in N^*\}$，输入数据可以是本域内的实体发来的数据，也可以是其他域实体发来的数据；$e.L$ 为本域内数据集合，$e.L=\{e.l_k\mid k\in N^*\}$；$e.\mathrm{Out}$ 为输出数据的集合，$e.\mathrm{Out}=\{e.\mathrm{out}_k\mid k\in N^*\}$；$e.F$ 为实体 e 对输入数据和本地数据进行的操作，包括读、写、主体行为等，$e.\mathrm{Out}=e.F(e.\mathrm{In},e.L)$；$e.G$ 为实体 e 对函数 $e.F$ 输出数据 $e.\mathrm{Out}$ 进行的传播操作，包括保存、备份、删除、转发等。

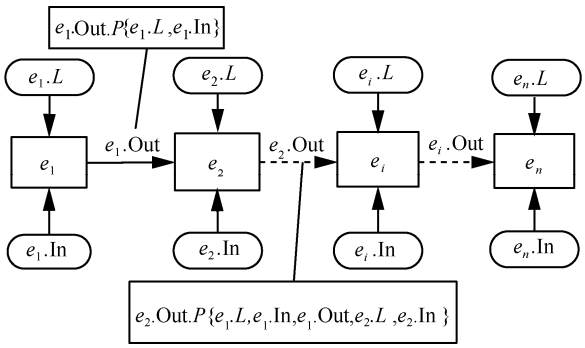

图 3 数据流模型

数据在不同实体之间的传播生成一个数据流（data flow）或数据传播链（data chain）。

定义 3 抽象的数据传播链 $<q_1,\cdots,q_i,\cdots,q_n>$，其中，$q_1$ 为数据传播链的起点，q_n 为数据传播链的终点，$q_i=<e_i.\mathrm{In},e_i.L,e_i.\mathrm{Out},e_i.F,e.G>$。其中，$e_i.\mathrm{In}$ 为第 i 个实体输入数据；$e_i.L$ 为第 i 个实体从本地数据容器中获得的数据资源；$e_i.\mathrm{Out}$ 为第 i 个实体输出数据，$e_i.\mathrm{Out}=e_i.F(e_i.\mathrm{In},e_i.L)$；$e_i.F$ 为第 i 个实体对数据进行的操作；$e_i.G$ 为第 i 个实体对输出数据 $e_i.\mathrm{Out}$ 进行的传播操作。

3.3 基于属性的访问控制模型

面向数据跨域流转的延伸访问控制机制中，基于实体属性和客体属性进行访问授权。

实体属性包括实体的通用属性、安全属性、环境属性。令实体 $\mathrm{EATT}=\{<\mathrm{eatt}^u,\mathrm{eatt}^s,\mathrm{eatt}^c>\ \mid\mathrm{eatt}^u\in\mathrm{EAtt}^U,\mathrm{eatt}^s\in\mathrm{EAtt}^S,\mathrm{eatt}^c\in\mathrm{EAtt}^C\}$。其中，$\mathrm{EAtt}^U$ 表示实体的通用属性集合，包括实体类别（人、软件、硬件）、实体角色、运行的平台等；EAtt^S 表示实体的安全属性集合，包括实体的安全等级、安全域等；EAtt^C 表示实体的环境属性集合，包括时间、位置等。

客体属性包括数据资源的通用属性、安全属性、环境属性。令客体 $\mathrm{OATT}=\{<\mathrm{oatt}^u,\ \mathrm{oatt}^s,\ \mathrm{oatt}^c>|\mathrm{oatt}^u\in\mathrm{OAtt}^U,\mathrm{oatt}^s\in\mathrm{OAtt}^S,\mathrm{oatt}^c\in\mathrm{OAtt}^C\}$。其中，$\mathrm{OAtt}^U$ 表示客体的通用属性集合，包括客体生成者、生成客体所进行的操作、客体起源数据等，客体起源数据用于表示客体生成过程中所有涉及的相关客体及其属性，客体 o 的起源数据

$o.P=\{<o_1,o_1.\text{att}>,<o_2,o_2.\text{att}>,\cdots,<o_n,o_n.\text{att}>\}$；$\text{OAtt}^S$ 表示客体的安全属性集合，包括客体的安全等级、安全域等；OAtt^C 表示客体的环境属性集合，包括客体生成的时间、设备等。

在进行延伸授权的访问控制时，除了考虑主体和客体属性外，还需要考虑数据容器的属性。令数据容器属性 $\text{DCATT}=\{<\text{dcatt}^u,\text{dcatt}^s,\ \text{dcatt}^c>|\ \text{dcatt}^u\in\text{DCAtt}^U,\ \text{dcatt}^s\in\text{DCAtt}^S,\text{dcatt}^c\in\text{DCAtt}^C\}$。其中，$\text{DCAtt}^U$ 表示数据容器的通用属性集合，包括数据容器位置、数据容器 IP 地址、数据库名、视图名等；DCAtt^S 表示数据容器的安全等级、安全域等；DCAtt^C 表示容器的环境属性集合。

面向数据跨域流转的延伸访问控制机制中，在实体和客体的众多属性中，有一部分属性是全局属性，如时间等；还有一部分属性是域内的局部属性，如位置、角色、身份等。域内的数据流转可以采用域内的局部属性直接进行访问控制，这样一方面可以保护隐私性，另一方面可以避免属性转化带来的空间和时间开销。在多域的环境中，跨域的访问控制是不可避免的。为了实现数据跨域安全流转和访问，每个域都存在一个或多个属性映射函数，实现域内属性与全局属性映射。在进行跨域访问时，例如 A 域数据流转到 B 域，首先调用 A 域的属性映射函数，将本域属性映射为全局属性，当数据流转到 B 域时，再调用 B 域的属性映射函数，将全局属性映射为 B 域的域内属性。这样每个域只需要维护本域与全局属性映射关系，提高了属性映射的效率，不同域间的属性互相不可知，降低了隐私泄漏的风险。

4　面向数据跨域流转的延伸访问控制机制

本文提出的面向数据跨域流转的延伸访问控制机制根据数据流转过程中的起源数据进行访问授权，并将访问控制分为约束访问控制和传播访问控制两类。约束访问控制主要解决实体在何种条件下能够对数据进行何种操作的问题，也就是控制上述数据传播链中 *e.F* 函数的操作。传播访问控制用于解决实体得到数据后，在何种条件下能进行何种传播操作的问题，也就是 *e.G* 函数的操作。通过约束访问控制和传播访问控制解决数据跨域延伸访问控制的问题。

4.1　约束访问控制

在约束访问控制中，实体可以进行操作集合 OP 主要包括读、写、主体行为，即 OP={read,write, useactions}。

权限 perms：实体到操作的映射。$\text{perms}=\{<e,\text{op}>|e\in E,\text{op}\in\text{OP}\}$。

授权函数 auth：根据实体属性、客体属性和对应的访问控制策略分配实体对应的权限。

$$\text{auth}=\text{perms}\times o=\{<e,\text{op},o>|e\in E,\text{op}\in\text{OP},o\in O\}$$

在判断实体对数据资源的读访问权限时，不仅考虑直接读权限，还需要考虑数据流转过程中所有涉及的数据间接读权限，即

$$\text{auth}(e,\text{read},o)\Leftrightarrow\text{auth}(e,\text{read},o)\wedge\text{auth}(e,\text{read},o.P)$$
$$\Leftrightarrow\text{auth}(e,\text{read},o)\wedge\text{auth}(e,\text{read},o_i.P),\ i=1,\cdots,n$$

其中，数据资源 o 的起源数据为 $o.P=\{<o_1,o_1.\text{att}>,<o_2,o_2.\text{att}>,\cdots,<o_n,o_n.\text{att}>\}$。

写操作与读操作类似，同样需要考虑数据流转过程中所有涉及的数据写权限，即

$$\text{auth}(e,\text{write},o)\Leftrightarrow$$
$$\text{auth}(e,\text{write},o)\wedge\text{auth}(e,\text{write},o.P)$$

用户行为（useactions）是实体对客体进行的一些特殊行为，如加密、签名、验签、计算摘要、隐私保护、噪声干扰等操作都属于用户行为。不同的操作对应的访问控制策略不同，在实际应用中，根据具体的行为类型和安全需求制定对应的访问控制策略。

4.2　传播访问控制

访问请求实体在得到数据访问权限后，数据的管理权和所有权就产生了分离。访问请求实体可以在本地任意留存、备份，留存的时间、备份的份数也没有限制；还可以将得到的数据任意转发给其他访问实体或系统。传播访问控制主要解决访问请求实体得到数据后进一步的权限管理问题，用于判断控制访问请求实体在得到数据的访问权限后，在什么条件下可以进一步对数据进行哪些传播操作。传播访问控制中，访问请求实体进行的操作集合主要包括保存、备份、删除、接收、发送、转发等操作，即 $\text{OP}=\{\text{save,backup,delete,receive,send, forward}\}$。

访问请求实体在得到数据访问授权后，将数据保存在数据容器 dc 中。在对保存操作进行访问控制判断时，不仅需要考虑访问请求实体是否对数据有保存的权限，还需要考虑保存数据的数据容器的属性是否满足数据保存的条件，以及保存的时间等。此外，还需要考虑整个数据流转过程中所有涉

及的数据保存权限。

$$\begin{aligned}&\text{auth}(e,\text{save},o,\text{dc},\text{time})\\&\Leftrightarrow \text{auth}(e,\text{save},o,\text{dc.att},\text{time})\wedge\\&\text{auth}(e,\text{save},o.P,\text{dc.att},\text{time})\\&\Leftrightarrow \text{auth}(e,\text{save},o,\text{dc.att},\text{time})\wedge\\&\text{auth}(e,\text{save},o_i.\text{dc.att},\text{time}),\ i=1,\cdots n\end{aligned}$$

其中，数据 o 的起源数据 $o.P=\{<o_1,o_1.\text{att}>,<o_2,o_2.\text{att}>,\cdots,<o_n,o_n.\text{att}>\}$；dc.att 指数据容器的属性，只有数据容器的属性满足保存条件时，数据容器才可以保存数据，例如只有数据容器安全等级大于或等于数据的安全等级时，才可以保存数据；time 表示数据在数据容器中保存的时间。

为防止数据丢失，经常将数据备份在数据容器中。

$$\begin{aligned}&\text{auth}(e,\text{backup},o,\text{dc},\text{time},\text{Number})\Leftrightarrow\\&\text{auth}(e,\text{backup},o,\text{dc.att},\text{time},\text{Number})\wedge\\&\text{auth}(e,\text{backup},o.P,\text{dc.att},\text{time},\text{Number})\end{aligned}$$

其中，Number 为备份的份数，Number=1 时可以省略不写。数据可以备份在不同的容器中，同一个容器可以备份多份数据。

对接收、保存和备份的数据资源，到了一定时间期限需要执行删除操作。

$$\begin{aligned}&\text{auth}(e,\text{delete},o)\Leftrightarrow\\&\text{auth}(e,\text{delete},o)\wedge\text{auth}(e,\text{delete},o.P)\end{aligned}$$

接收操作涉及不同实体之间数据流转以及流转的路径。在进行访问控制时，不仅要考虑数据本身和接收数据的实体，还需要考虑发送数据的实体、发送的方式和经过的路径等因素，同时还需要考虑数据流转过程中所有涉及的数据。接收操作可表示为

$$<e_{i+1},e_i,\text{receive},e_i.\text{Out},e_i.\text{manner},e_i.\text{path}>$$

其中，e_i.Out 表示第 i+1 个实体接收第 i 个实体输出的数据资源；e_i.manner 为接收的方式，$e_i.\text{manner}\in\text{MANNER}$，MANNER 为数据传输的方式，可以通过网络传输，也可以通过光盘、U 盘或纸质文件传输；e_i.path 为发送的路径，$e_i.\text{path}\in\text{PATH}$，PATH 为数据传输的路径集合，包括数据在不同网络节点传播时形成的传播路径，或通过光盘、U 盘或纸质文件传输等人工传播时形成的传播路径。

$$\begin{aligned}&\text{auth}(e_{i+1},e_i,\text{receive},e_i.\text{Out},e_i.\text{manner},e_i.\text{path})\Leftrightarrow\\&\text{auth}(e_{i+1},e_i,\text{receive},e_i.\text{Out},e_i.\text{manner},e_i.\text{path})\wedge\\&\text{auth}(e_{i+1},e_i,\text{receive},e_i.\text{Out}.P,e_i.\text{manner},e_i.\text{path})\end{aligned}$$

其中，e_i.Out.P 为第 i 个实体输出的数据 e_i.Out 的起源数据。

对于发送操作同样要考虑发送数据的实体、发送的方式、经过的路径、接收的实体以及数据流转过程中所有涉及的数据。第 i 个实体将自己输出的数据资源 e_i.Out 发送给第 i+1 个实体的发送操作可表示为

$$<e_i,e_{i+1},\text{send},e_i.\text{Out},e_i.\text{manner},e_i.\text{path}>$$

其中，e_i.manner 为发送的方式，e_i.path 为发送的路径。

$$\begin{aligned}&\text{auth}(e_{i+1},e_i,\text{send},e_i.\text{Out},e_i.\text{manner},e_i.\text{path})\Leftrightarrow\\&\text{auth}(e_{i+1},e_i,\text{send},e_i.\text{Out},e_i.\text{manner},e_i.\text{path})\wedge\\&\text{auth}(e_{i+1},e_i,\text{send},e_i.\text{Out}.P,e_i.\text{manner},e_i.\text{path})\end{aligned}$$

如果发送的数据是从上一个实体转发来的，在进行转发控制时，需要增加转发的次数。转发操作表示为

$$\begin{aligned}&<e_i,e_{i+1},\text{forward},e_i.\text{Out},e_i\text{manner},\\&e_i.\text{path},\text{forwardNumber}>\end{aligned}$$

数据转发时，需要判断转发次数是否超过上界，转发成功后，转发次数加 1。

$$\begin{aligned}&\text{auth}(e_{i+1},e_i,\text{forward},e_i.\text{Out},e_i.\text{manner},e_i.\text{path})\Leftrightarrow\\&\text{auth}(e_{i+1},e_i,\text{forward},e_i.\text{Out},e_i.\text{manner},e_i.\text{path})\wedge\\&(\text{forwardNumber}\leqslant\text{forwardMax})\wedge\\&\text{auth}(e_{i+1},e_i,\text{forward},e_i.\text{Out}.P,e_i.\text{manner},e_i.\text{path})\wedge\\&(\text{forwardNumber}_i\leqslant\text{forwardMax}_i),\ i=1,\cdots,n\end{aligned}$$

在对数据进行跨域延伸的访问控制时，对于域内流转直接采用域内的属性进行授权判断；对于跨不同域的数据流转通过属性映射函数实现域内属性全局属性的映射，进而实现域间不同实体和客体的属性映射，提高访问控制效率，降低隐私泄露的风险。

4.3 安全性分析

现有访问控制机制重点考虑访问请求实体 e 得到数据资源 o 前的访问权限的控制。当访问请求实体 e 得到数据资源 o 后，资源所有者就失去了对数据资源 o 的控制权限，访问请求实体 e 可以对数据资源 o 进行任意操作，如保存、备份、删除等操作，

甚至转发给其他访问请求实体，例如访问请求实体 e 转发给 e_1，e_1 再转发给 e_2，不同实体之间任意转发造成资源的任意扩散。为解决上述问题，本文提出的跨域延伸访问控制机制从约束控制和传播控制 2 个方面进行访问控制，不仅考虑读、写等操作，还进一步考虑访问请求实体得到资源后延伸控制，分别从保存、备份、删除、转发等操作进行细粒度延伸控制。在对保存和备份操作进行控制时，不仅考虑实体对资源是否有保存的权限，同时考虑保存的容器属性是否满足条件。对资源备份时，还需要考虑备份的份数等条件。对于转发操作，不仅考虑发送实体和接收实体，同时考虑资源转发的路径、方式和次数，保证资源在受控的实体范围内通过受控的方式和平台进行消息发布和共享。利用延伸授权的访问控制机制有效解决了上述数据资源在不同实体之间任意扩散的情况。同时，在实体得到数据资源后，也不可以对数据资源任意修改、删除和保存，有效限制了数据资源在传播过程失真的情况。文献[8]分别从发送和接收 2 种不同操作限制数据传播，在一定程度上解决了数据流转过程中的访问控制问题，但该文献只考虑发送和接收 2 个单独动作，没有考虑数据整个流转过程，对数据在不同实体之间的多次转发造成的泄露问题不能有效解决。

另一方面，现有访问控制重点考虑对数据资源 o 的直接访问控制，但数据资源 o 通常由不同实体通过对不同数据资源进行各种不同操作得到。假设数据资源 o 由实体 e_1、e_2、e_3 分别对数据资源 o_1、o_2、o_3 进行不同操作得到。假设实体 e 有对数据资源 o 读的访问权限，但对数据资源 o_1、o_2 没有读的权限，而资源 o 是由 o_1、o_2 组成的，那么 e 通过 o 得到了 o_1、o_2 的读权限，导致数据资源 o_1、o_2 的间接泄露。本文利用数据传播链（或者数据流）记录了数据的起源信息，在进行访问控制判断时，不仅判断对数据资源本身是否有访问权限，同时考虑对整个数据传播链中所有参与数据资源的生成和传播的数据资源和实体的访问权限，有效降低了数据资源在不同实体之间流转造成的间接泄露风险。文献[15]利用 OPM（open provenance model）记录起源数据，并利用起源数据进行访问控制判断，但存在起源数据过于复杂，并且在数据跨域流转过程中由于起源数据过于复杂导致访问控制效率低。本文利用数据传播链（或者数据流）记录了数据的起源数据，不考虑数据生成过程中不同实体对数据组成部分进行的操作以及不同实体与数据组成部分的关系，简化了起源数据，提高了访问控制效率。

5　用例分析

本节通过电子发票全生命周期的流转过程给出数据跨域流转延伸访问控制机制的实现方法。

5.1　电子发票数据流分析

电子发票数据流转过程如图 4 所示，共有 6 个实体。

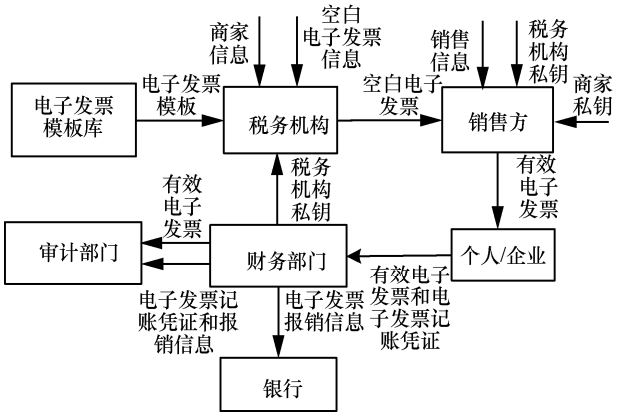

图 4　电子发票数据流转过程

税务机构(e_1)。税务机构从电子发票模板库中提取要颁发的电子发票模板($e_1.\text{in}_1$)，然后生成空白发票的 ID 号、有效期等相关数据 $e_1.l_1$，以及销售方名称等销售方的相关数据 $e_1.l_2$。为了保证空白发票的合法性，税务机构使用自己的私钥 $sk_{e_1}=e_1.l_3$ 调用签名算法 sig，对空白发票相关数据 $(e_1.\text{in}_1\|e_1.l_1\|e_1.l_2)$ 进行签名，得到税务机构的签名 $\text{sig}_{e_1}(e_1.l_4),\text{sig}_{e_1}=\text{sig}(\text{sk}_{e_1}, e_1.\text{in}_1\|e_1.l_1\|e_1.l_2)$。税务机构将空白发票相关数据和税务机构签名一起生成空白电子发票 $e_1.\text{out}$，$e_1.\text{out}=e_1.\text{in}_1\|e_1.l_1\|e_1.l_2\|e_1.l_4$，并将生成的空白电子发票发送给销售方。

销售方(e_2)。销售方得到税务机构颁发的空白电子发票 $e_1.\text{out}$ 后，首先使用税务机构的公钥 $\text{pk}_{e_1}(e_2.\text{in}_1)$调用签名验证算法 verify 验证税务机构的签名，即 $\text{verify}(\text{pk}_{e_1}, e_1.\text{out})$，验证通过说明该空白发票为合法发票。销售方生成销售数据 $e_2.l_1$，为了保证销售数据的真实性，销售方使用自己的私钥 $\text{sk}_{e_2}=e_2.l_2$ 调用签名算法对销售数据和空白电子发票进行签名，得到销售方的签名 $\text{sig}_{e_2}(e_2.l_3)$，$e_2.l_3=\text{sig}_{e_2}=\text{sig}(\text{sk}_{e_2}, e_2.l_1\|e_1.\text{out})$。销售方将空白电

子发票、销售数据、销售方签名一起生成有效电子发票 $e_2.\text{out} = e_1.\text{out} \| e_2.l_1 \| e_2.l_3$，发送给买方（个人/企业）。

个人/企业(e_3)。个人/企业得到有效电子发票 e_2.out 后，首先使用税务机构的公钥 $\text{pk}_{e_1}(e_3.\text{in}_1)$和销售方公钥 $\text{pk}_{e_2}(e_3.\text{in}_2)$验证电子发票的合法性和真实性，即 $\text{verify}(\text{pk}_{e_1}, e_1.\text{out})$与 $\text{verify}(\text{pk}_{e_2}, e_2.\text{out})$。验证通过后，根据电子发票生成电子发票记账凭证 $e_3.l_1$，并将有效电子 e_2.out 和电子记账凭证 $e_3.l_1$ 一起发送给财务部门进行报销，即 $e_3.\text{out} = e_2.\text{out} \| e_3.l_1$。

财务部门(e_4)。财务部门根据有效电子发票 e_2.out 和电子记账凭证 $e_3.l_1$ 对电子发票进行报销，并生成账单数据 $e_4.l_1 = e_4.\text{out}_1$ 发送给银行；根据下一步银行生成的划账数据 $e_5.\text{out} = e_4.\text{in}_1$ 生成电子发票报销数据 $e_4.l_2$，并将有效电子发票 e_2.out、电子记账凭证 $e_3.l_1$ 和电子发票报销数据 $e_4.l_2$ 存档保存，根据需要接受审计部门的审查。

银行(e_5)。银行根据财务部门生成的账单数据 $e_4.l_1 = e_4.\text{out}_1$ 对个人/企业划账，生成电子发票划账数据 e_5.out，发送给财务部门。

审计部门(e_6)。审计部门从财务部门调取电子发票、电子发票记账凭证和电子发票报销 $e_4.\text{out}_2$，$e_4.\text{out}_2 = e_2.\text{out} \| e_3.l_1 \| e_4.l_2$，进行财务审计，生成审计结果 e_6.out。

电子发票模板库是一个数据容器，存放各种电子发票模板。税务机构根据需要从电子发票模板库调用电子发票模板。

为简化，本文假设税务机构属于域 A，销售方都属于域 B，个人/企业和各自的财务部门属于域 C，银行属于域 D，审计机构属于域 E，假设电子发票流转过程中，所有的实体已经完成了身份认证。

5.2 电子发票流转中的访问控制需求和访问控制策略

下面从电子发票流转过程中的访问控制需求解释数据跨域延伸的访问控制机制的实施方法。

约束访问控制需求。在上述电子发票流转过程中，各个实体对输入数据和本地数据有读和写的需求。如税务机构对电子发票模板和税务机构私钥有读的需求；销售方需要根据空白电子发票、销售数据和销售方的签名生成有效电子凭据，销售方有对上述数据写的需求。此外，各个实体有进行主体行为的需求，如税务机构需要对空白电子发票进行签名，电子发票流转过程中的主体行为包括签名和验证签名、生成销售数据和电子记账凭证等。

传播访问控制需求。各个实体在得到数据后还需要进一步进行传播操作，如各个实体有接收输入数据的需求，对生成的输出数据有发送需求。部分实体对输入数据和生成的数据有保存的需求，比如销售方从税务机构拿到空白的电子发票后有保存的权限，但保存空白电子发票的数据容器有一定安全要求，空白电子发票只能保存在特殊的数据容器内。空白电子发票有一定的使用期限，超过使用期限，销售方需要将空白电子发票返还给税务机构，而且销售方没有备份空白电子发票的权限。

针对上述约束访问控制需求和传播访问控制需求，生成下述约束访问控制策略和传播访问控制策略。

1) 约束访问控制

根据约束访问控制，电子发票流转过程中各个实体读和写的访问控制策略为

$$\text{auth}(e, \text{read}, o) \Leftrightarrow$$
$$\text{auth}(e, \text{read}, o) \wedge \text{auth}(e, \text{read}, o.P)$$
$$\text{auth}(e, \text{write}, o) \Leftrightarrow$$
$$\text{auth}(e, \text{write}, o) \wedge \text{auth}(e, \text{write}, o.P)$$

进行读、写访问授权判断时，不仅需要判断直接访问权限，还需要根据起源数据判断间接访问权限。

本实例中的主体行为主要涉及签名和验签操作。在执行签名和验签操作前，访问请求实体对所有输入数据有读权限、对输出数据有写权限。

2) 传播访问控制

在传播访问控制中，接收和发送的访问控制策略为

$$\text{auth}(e_{i+1}, e_i, \text{send}, e_i.\text{out}, e_i.\text{manner}, e_i.\text{path}) \Leftrightarrow$$
$$\text{auth}(e_{i+1}, e_i, \text{send}, e_i.\text{out}, e_i.\text{manner}, e_i.\text{path}) \wedge$$
$$\text{auth}(e_{i+1}, e_i, \text{send}, e_i.\text{out}.P, e_i.\text{manner}, e_i.\text{path})$$
$$\text{auth}(e_{i+1}, e_i, \text{receive}, e_i.\text{out}, e_i.\text{manner}, e_i.\text{path}) \Leftrightarrow$$
$$\text{auth}(e_{i+1}, e_i, \text{receive}, e_i.\text{out}, e_i.\text{manner}, e_i.\text{path}) \wedge$$
$$\text{auth}(e_{i+1}, e_i, \text{receive}, e_i.\text{out}.P, e_i.\text{manner}, e_i.\text{path})$$

保存和备份对应的访问控制策略为

$$\text{auth}(e_{i+1}, \text{save}, e_i.\text{out}, \text{dc}, \text{time}) \Leftrightarrow$$
$$\text{auth}(e_{i+1}, \text{save}, e_i.\text{out}, \text{dc.att}, \text{time}) \wedge$$
$$\text{auth}(e_{i+1}, \text{save}, e_i.\text{out}.P, \text{dc.att}, \text{time})$$

$$\text{auth}(e_{i+1},\text{backup},e_i.\text{out},\text{dc},\text{time},\text{Number}) \Leftrightarrow$$
$$\text{auth}(e_{i+1},\text{backup},e_i.\text{out},\text{dc.att},\text{time},\text{Number}) \wedge$$
$$\text{auth}(e_{i+1},\text{backup},e_i.\text{out}.P,\text{dc.att},\text{time},\text{Number})$$

5.3　电子发票流转实例

本节通过销售方保存空白电子发票，财务部门接收、保存、备份有效电子发票和电子记账凭证具体实例，详细解释传播控制访问控制中保存、接收操作的访问控制实现。

销售方将空白电子发票保存在自己的数据容器 dc_2 中，销售方保存空白电子发票的访问控制策略可以表示为

$$\text{auth}(e_2,\text{save},e_1.\text{out},\text{dc}_2,\text{time}) \Leftrightarrow$$
$$\text{auth}(e_2,\text{save},e_1.\text{out},\text{dc}_2.\text{att},\text{time}) \wedge$$
$$\text{auth}(e_2,\text{save},e_1.\text{out}.P,\text{dc}_2.\text{att},\text{time})$$

其中，dc_2.att 保存空白电子发票的数据容器的属性，假设规定只有安全等级大于 2 级的数据容器才可以保存空白电子发票，那么销售方要保存空白电子发票，需要 dc_2.att.securitylevel>2。假设空白电子发票的有效期为$[t_1,t_2]$，在有效期内销售方才可以保存空白电子发票；如果不在有效期内，销售方将保存的空白电子发票返回给税务机构。

财务部门接收个人或企业有效电子发票和电子记账凭证 $e_3.\text{out} = e_2.\text{out} \| e_2.l_1$，审核通过后对有效电子发票进行报销。财务部份接收有效电子发票和电子记账凭证的访问控制策略为

$$\text{auth}(e_4,e_3,\text{receive},e_3.\text{out},e_3.\text{manner},e_3.\text{path}) \Leftrightarrow$$
$$\text{auth}(e_4,e_3,\text{receive},e_3.\text{out},e_3.\text{manner},e_3.\text{path}) \wedge$$
$$\text{auth}(e_4,e_3,\text{receive},e_3.\text{out}.P,e_3.\text{manner},e_3.\text{path})$$

其中，有

$$e_3.\text{out}.P = \{<e_1.\text{in}_1,e_1.\text{in}_1.\text{att}>,<e_1.l_1,e_1.l_1.\text{att}>,$$
$$<e_1.l_2,e_1.l_2.\text{att}>,<e_1.l_3,e_1.l_3.\text{att}>,<e_1.l_4,e_1.l_4.\text{att}>,$$
$$<e_2.l_1,e_2.l_1.\text{att}>,<e_2.l_2,e_2.l_2.\text{att}>,<e_2.l_3,e_2.l_3.\text{att}>\}$$

在数据接收时，需要考虑数据传送的方式和传送的路径。比如，有的财务部门规定只能使用域内网络进行相关数据的发送和接收，财务部门在接收数据时，可以拒绝接收通过外网发送来的有效电子发票和电子记账凭证。本文假设个人或企业和财务部门属于同一个安全域，在进行数据发送和接收时，不需要进行属性的映射，可以直接使用域内属性进行访问控制判断。财务部门把相关数据发送给银行或审计部门时，其属于不同的安全域，需要进行跨域的属性映射，可以通过全局属性映射实现域间不同实体和客体的属性映射。

报销结束后，财务部门会对 e_3.Out 进行保存和备份。假设财务部门将有效电子发票和电子记账凭证保存和备份在自己的数据容器 dc_4 中，且只备份一份。财务部门保存有效电子发票和电子记账凭证的访问控制策略为

$$\text{auth}(e_4,\text{save},e_3.\text{out},\text{dc}_4,\text{time}) \Leftrightarrow$$
$$\text{auth}(e_4,\text{save},e_3.\text{out},\text{dc}_4.\text{att},\text{time}) \wedge$$
$$\text{auth}(e_4,\text{save},e_3.\text{out}.P,\text{dc}_4.\text{att},\text{time})$$

备份有效电子发票和电子记账凭证的访问控制策略为

$$\text{auth}(e_4,\text{backup},e_3.\text{out},\text{dc}_4,\text{time}) \Leftrightarrow$$
$$\text{auth}(e_4,\text{backup},e_3.\text{out},\text{dc}_4.\text{att},\text{time}) \wedge$$
$$\text{auth}(e_4,\text{backup},e_3.\text{out}.P,\text{dc}_4.\text{att},\text{time})$$

对于备份多份的情况，可以对不同的数据容器采用上述策略单独考虑。

6　结束语

数据跨系统跨域流转已成为复杂网络环境中数据共享的趋势，如何确保数据跨系统跨域流转后的受控共享是访问控制的重大挑战。现有访问控制机制主要解决访问请求前的访问控制问题，而对于访问请求实体得到访问权限后进一步延伸控制的研究很少。针对上述问题，本文提出了面向数据跨域流转的延伸访问控制机制，将访问控制分为约束访问控制和传播访问控制 2 类，根据数据流转过程中的起源数据进行访问授权，解决数据跨域共享延伸授权的问题。安全性和性能分析表明，所提机制解决了数据跨域流转过程中的延伸控制问题，在保证安全性的前提下，有效提高了访问控制的效率，并通过电子发票全生命流转过程展示了数据跨域流转的延伸访问控制机制实施方法。

未来还需要在以下方面进一步研究：结合不同的应用背景，给出面向数据跨域流转的延伸访问控制机制实施方法和访问控制执行效率优化措施。

参考文献：

[1] MYERS A C. JFlow: practical mostly-static information flow control[C]// Symposium on Principles of Programming Languages. 1999:228-241.

[2] MYERS A C, LISKOV B. A decentralized model for information flow control[J]. ACM SIGOPS Operating Systems Review, 1997,

31(5):129-142.
[3] KROHN M, YIP A, BRODSKY M, et al. Information flow control for standard OS abstractions[C]// The 21st ACM SIGOPS Symposium on Operating Systems Principles. 2007:321-334.
[4] DOROTHY E. A lattice model of secure information flow[J]. Communications of ACM, 1976, 19(5):236-243.
[5] BELL D E, LAPADULA L J. Secure computer system: unified exposition and multics interpretation, MTR-2997 Rev. 1 [R]. Bedford, CA: MITRE Corporation, 1976.
[6] BIBA K J. Integrity considerations for secure computer systems[R]. USA: USAF Electronic Systems Division Mitre Corp Bedford MA, 1977.
[7] ZELDOVICH N, BOYD-WICKIZER S. Securing distributed systems with information flow control[C]// USENIX Symposium on Networked Systems Design and Implementation. USENIX Association, 2006:293-308.
[8] SHE W, YEN I L, BASTANI F, et al. Role-based integrated access control and data provenance for SOA based net-centric systems[J]. IEEE Transactions on Services Computing, 2016, 9(6):940-953.
[9] SHE W, YEN I L, THURAISINGHAM B, et al. Security-aware service composition with fine-grained information flow control[J]. IEEE Transactions on Services Computing,2013, 6(3):330-343.
[10] ASUQUO P, CRUICKSHANK H, OGAH C P A, et al. A distributed trust management scheme for data forwarding in satellite DTN emergency communications[J]. IEEE Journal on Selected Areas in Communications, 2018, PP(99):1.
[11] LI Q, SANDHU R, ZHANG X, et al. Mandatory content access control for privacy protection in information centric networks[J]. IEEE Transactions on Dependable & Secure Computing, 2017, PP(99):1.
[12] GROEF W D, DEVRIESE D, NIKIFORAKIS N, et al. FlowFox: a Web browser with flexible and precise information flow control[C]// The 2012 ACM conference on Computer and Communications Security(CCS) . ACM, 2012:748-759.
[13] SHE W, YEN I L, THURAISINGHAM B, et al. The SzCIFC model for information flow control in Web service composition[C]//IEEE International Conference on Web Services. 2009:1-8.
[14] SHE W, YEN I L, THURAISINGHAM B, et al. Policy-driven service composition with information flow control[C]// IEEE International Conference on Web Services. 2010:50-57.
[15] PARK J, DANG N, SANDHU R. A provenance-based access control model[C]// Tenth International Conference on Privacy, Security and Trust. 2012:137-144.
[16] SUN L, PARK J, SANDHU R. Engineering access control policies for provenance-aware systems[C]// The Third ACM Conference on Data and Application Security and Privacy(COPASPY). ACM, 2013: 285-292.
[17] SUN L, PARK J, DANG N, et al. A provenance-aware access control frame work with typed provenance[J]. IEEE Transactions on Dependable & Secure Computing, 2016, 13(4):411-423.
[18] 李凤华, 王彦超, 殷丽华,等. 面向网络空间的访问控制模型[J]. 通信学报, 2016, 37(5):9-20.
LI F H, WANG Y C, YIN L H, et al. Novel cyberspace-oriented access control model[J]. Journal on Communications, 2016, 37(5):9-20.

[作者简介]

谢绒娜（1976− ），女，山西永济人，西安电子科技大学博士生，主要研究方向为网络与系统安全、访问控制、密码工程。

郭云川（1977− ），男，四川营山人，博士，中国科学院信息工程研究所副研究员、博士生导师，主要研究方向为访问控制、形式化方法。

李凤华（1966− ），男，湖北浠水人，博士，中国科学院信息工程研究所研究员、博士生导师，主要研究方向为网络与系统安全、信息保护、隐私计算。

史国振（1974− ），男，河南济源人，博士，北京电子科技学院副教授、硕士生导师，主要研究方向为网络与系统安全、嵌入式安全。

王亚琼（1994− ），女，山西朔州人，西安电子科技大学硕士生，主要研究方向为访问控制与网络安全。

耿魁（1989− ），男，湖北红安人，博士，中国科学院信息工程研究所助理研究员，主要研究方向为网络安全。