基于无线传输网络中隐私保护的访问控制机制

宋　欢

湖北邮电规划设计有限公司 湖北 武汉 430024

【摘　要】：近几年，随着无线网络在医疗、军事、商业等领域的不断发展，越来越受到人们的关注。随着无线通讯技术的发展，电子商务、电子政务、战术互联网等领域的发展将会有很大的发展空间，但是由于无线网络的开放性，使得数据的传送受到了被动监听、数据拦截、隐私入侵等攻击。尤其是由于节点资源的限制，采用具有高运算能力和高通讯代价的安全机制是不现实的，所以本文对无线网络的安全问题进行了深入的探讨。在这些服务中，访问控制是一个非常关键的安全服务，它可以保证合法使用者的权限，同时也可以阻止非授权使用者的非法进入。因此，本论文所研究的无线传输网络中隐私保护的访问控制机制对于无线网络的安全性有很大的理论和实际意义。

【关键词】：无线网络；隐私保护；访问控制机制

Access Control Mechanism Based on Privacy Protection in Wireless Transmission Network

Huan Song

Hubei Post and Telecommunications Planning and Design Co., Ltd. Hubei Wuhan 430024

Abstract: In recent years, with the continuous development of wireless network in medical, military, commercial and other fields, more and more attention are received. With the development of wireless communication technology, the development of e-commerce, e-government, tactical Internet and other fields will have a great space for development, but due to the openness of wireless network, data transmission by passive monitoring, data interception, privacy intrusion and other attacks. Especially due to the limitation of node resources, it is unrealistic to adopt the security mechanism with high computing power and high communication cost, so this paper discusses the security problem of wireless network deeply. Among these services, access control is a very critical security service that guarantees the rights of legitimate users and also prevents unauthorized entry by unauthorized users. Therefore, the access control mechanism of privacy protection in wireless transmission networks studied in this paper has great theoretical and practical significance for the security of wireless networks.

Keywords: Wireless network; Privacy protection; Access control mechanism

引言

在信息时代飞速发展的今天，无线网络的广泛使用与运用，让人们的感知与通讯不再受到时间、空间、对象的限制，随时随地都能获得网络资源与服务，大大改善了人们的生活品质与工作品质，可以说，无线网络推动了整个社会的发展。与有线网络相比，无线网络具有更灵活的组网方式、节省频谱和功率，以及网络规模的升级和发展。利用无线通讯技术实现了数据采集、汇聚、协同感知、传输和处理等功能，使得用户可以方便地获得所需要的数据。近十年来，随着互联网的飞速发展，无线通讯的基础建设和各种业务不断地发展，以适应社会的不断发展。还有一些报告指出，由于非法网络犯罪，包括恶意攻击，黑客，数据伪造，非法访问，财务信息窃取，网络攻击/追踪等越来越多[1]。随着人们利用无线网络（例如蜂窝网络、Wi-Fi）进行在线银行业务频繁的情况下，增强无线通信的安全性，保护个人隐私，是无线网络研究和应用的一个关键环节。

1 大数据时代网络隐私信息存在隐患

随着大数据时代的来临，社会信息化进程加快，同时也给社会网络的信息安全造成了威胁。

（1）在大数据时代，存在着许多特征。其特征之一是资料资讯的开发、扩充和快速地散布。通过各种搜索引擎、社交软件、APP 等渠道，很多人都可以轻松地获得个人信息，例如，腾讯 QQ，微信，微博等社交网站。三个社交网站注册的时候，注册的条件都不一样，比如邮箱、手机号、真实姓名等，还有联系方式、兴趣爱好、生日、地区、身份证等。这也是一种暴露自己的秘密的风险。

（2）在大数据时代，个人隐私的泄漏通常是在互联网上挖掘、结合、预测等方法，产生一个相对完整的个体信息。比如，通过微信、政府机构、组织等社交网站，收集了大量的个人信息和个人的隐私，通过收集的数据和聊天记录，可以了解到一个人的生活习惯、爱好、消费水平、收入状况、工作性质、居住城市、经济状况等。事实上，在央视 315 晚会上，披露了大量的信息技术窃取个人资料的录像，令全国人民大为震惊[2]。海量资讯科技，国内所有车主资料，各大银行客户资料，乃至股民资料，一应俱全，价格更是便宜到了极点。所以，在大数据时代，人们可以通过社会化网络平台获取“1+1>2”的个人和私人信息。

（3）个人资料或个人隐私应经本人同意后才能公开或使用。这种形式在大数据时代发生了根本性的变化。个人信息和隐私的“二次使用或开发”自然而然地成为主流，这种做法对个人信息和隐私权的保护极其不安全。

因此，在大数据时代，社交网络的隐私保护仍然存在一定的缺陷。在大数据时代，如何有效完善网络隐私安全机制成为社交网络的一个重要任务。

2 访问控制机制概述

当前访问控制机制的研究主要包括传统访问控制机制、基于角色访问控制机制以及基于信任访问控制机制。传统的访问控制机制有自助访问控制机制和强制访问控制机制（如军队）。

2.1 自主访问控制技术

自主访问控制机制中的自主性，是指主体根据自身对安全政策的了解或意愿，可以向其他用户授予、撤销或收回对目标的访问权限，并将其转让给其他用户。自主访问控制是一种较为灵活的数据存取方式，在商用等领域有着广泛的应用。但是它的安全性不高，一旦用户将访问的权限转移到其他地方，就会导致安全问题的进一步恶化，而且权限管理也会变得更加复杂，不利于统一管理，不适合在复杂的网络中使用。

2.2 强制访问控制技术

强制访问控制是一种多级安全的强制控制策略，其特征在于，主、客体之间的安全等级是独立的，并通过授权单位或系统管理员来划分主体的信任程度和对象的信息敏感性。使用者无法更改被预先指定的可信级别、存取权限和目标资源的安全性。根据所掌握的权限，根据资源的安全性等级，对不同使用者层级的使用者进行存取。访问控制是一种对权限进行严格的集中控制，这是针对军队等对安全等级有很高要求的地方。强制访问控制管理是一种非常严格、高度集中的管理方式，其管理工作量巨大、不灵活，不适合在用户数量多、资源种类多的情况下使用[3]。

2.3 基于角色的访问控制

以角色为基础的访问控制主要引入角色概念。角色是使用者与权限之间的代理层，代表使用者与权限之间的存取权限关系。通过授予角色访问权限代替用户或组。根据用户在系统中所扮演的角色，根据用户的权限进行相应的资源操作，方便管理，同时，根据最低的权限，用户可以执行特定的任务，而不会因为权限过大而影响系统的安全性。基于角色的访问控制机制通过静态授权角色，用户可以获得相应的资源访问权限，这是一种很难实现的机制，而且很多角色模型和算法还处于研究阶段，很难在实践中应用。

针对开放网络环境中各主体之间的互动和资源的不确定，本文提出的三种方法更适合于在密闭的网络中使用。而对于服务对象的合法性以及服务提供者所提供的服务的安全，则是对传统访问控制体制的一个重要挑战。由于开放网络服务于多个使用者、多个领域的存取问题，单凭单一的存取方式无法满足最大的安全性要求。一个系统的安全战略是由几种访问控制或几种不同的控制方法组合而成。

3 网络隐私保护的访问控制

3.1 网络数据访问控制面临的问题

网络计算和云存储技术的开放性、数据托管状态、数据安全的多元化管理，都给网络数据安全带来了挑战。为了解决上述问题，网络访问控制的研究不仅要确保云端资源和服务能够被合法的使用者访问和利用，还要兼顾隐私保护、安全创建和可信自毁[4]。因此，网络数据访问控制所面对的挑战有以下几点：

（1）数据的可用性，是指用户可以通过不同的终端设备、不同的访问方式，随时访问网络资源，既方便了用户的使用，又带来了访问的随机性和不可控制的问题。此外，由于网络数据的多元素化、安全管理的多元化，使得网络计算必须解决多要素、多层次管理的问题。

（2）网络计算的数据类型多种多样：包括图像、音频、视频、文本等多种类型。一些资源需要具有访问控制的细粒度和访问控制的对象化管理。通常，数据都是经过加密的，然后上传到网络中；同时，在建立访问控制条件和权限的细节描述时，也要建立相应的数据。

（3）访问策略应当是动态的、多变的，应当与资源的生命周期相结合的，而在不同的生命周期中，资源的策略、访问权限和用户的需求也是不同的。由于用户的随机性、多要素和多层次的管理，使得网络计算的访问控制策略必须具有与数据的生命周期相结合、动态调整等特征。

（4）网络计算的开放和共享特性使每一个网络应用都具有各自的安全管理领域，并对各自的资源和使用者进行管理。在跨区域访问资源时，需要对域边界进行认证，需要对用户进行统一的身份验证。在跨领域资源的存取过程中，各安全领域都有各自的访问控制策略，因此，在跨领域的资源共享与保护上，必须遵守共同的、双方都认可的安全策略。因此，网络安全技术的访问控制策略应当是多种安全策略的综合，新的综合策略在保证安全的同时，也不能违反原有安全管理领域的访问控制策略。

（5）使用者与网络端服务商的互不信赖。使用者将资料移交至网络端服务商进行管理，其所有权与管理权被分开，使用者与服务器不再处于相同的受信赖范围内。使用者作为用户的身份访问服务器，使用者并不完全相信服务器，或是资料的安全不受使用者控制，使用者资料会遭到公司员工非法泄漏、篡改、盗用。此外，一旦取得了法定的身份，所进行的违法或

恶意的攻击或破坏，都会对网络端服务平台构成极大的危害。为了提高网络的安全性和可靠性，必须在网络中引进可信的概念。

综合上述网络访问控制的需求，认为其安全策略应当是具有多层次安全策略、动态、自适应、具有细粒度访问控制和目标化管理的特点，所以网络安全控制策略必须是综合性的访问控制机制，从而保障网络计算的安全。

4 网络隐私保护访问控制机制

由于网络环境具有开放、共享的特点，传统的安全控制策略已经不能很好地解决这些问题，因此，如何在网络环境中推广应用多种传统的控制机制以及不同的安全控制策略语言。关于网络的访问控制机制，目前学术界的研究主要集中在基于身份的、属性的、加密的、多级的、分布的、跨领域等等。

基于身份的访问控制机制主要是针对分布式开放式网络中的细粒度访问，以确保网络的安全性，但是随着网络计算平台的不断发展，以及混合访问控制的融合，必然会给基于身份的访问控制提出新的挑战。基于特征的访问控制是在基于身份的访问控制的基础上的一种扩展和发展，它在满足现有的优点的前提下，能够解决各种情况下的访问控制机制，具有一定的理论和研究价值。

密码技术是利用特定的算法和密钥对数据进行加密，从而达到保护数据的保密目的，将加密后的数据存储到云端服务器中，从而达到与访问控制策略机制的互补。访问控制机制是以加密算法为基础的。

目前，多层次安全访问控制机制的研究包括基于行为的多层次安全访问控制模型，其重点是在背景信息中缺少时间、环境状况（空间状态）等。在此基础上，可以将传统的安全访问控制与基于行为的访问控制模型结合，定义该模型的多层安全性；针对用户的权限随时可能改变的动态扩展需求，提出了安全的读写请求，定义了行为的读写安全级别，利用行为属性映射功能，在一定的时间和空间条件下，利用行为属性映射功能，获得安全属性，确定安全规则，以确保动态调节的时间和空间需求；与传统 BLP 相比，基于行为的多层安全访问控制模型在空间和时间上都表现出更大的灵活性。

在分布式和域的访问控制模型下，存在多个域，各域具有客户、服务器、域安全管理、域安全管理程序。协作和跨区存取是分布体系中普遍存在的一种行为，也是一个很大的特点。基于这一模型，出现了基于角色的分布式访问控制模型、基于域的访问控制模型以及利用控制模型来处理跨域和分散的管理员协作问题。

5 无线传输网络中隐私保护的访问控制机制发展趋势

在无线通信领域，访问控制技术的发展是非常具有挑战性的。访问控制是一种必要的安全措施，它可以阻止非法进入无线网络的恶意使用者，特别是医疗和军事方面。所以，对访问控制机制进行深入的研究，无论是在理论上还是在实践上都有着重要的意义。目前研究访问控制机制的基础上，还有一些不足之处，如：

（1）当前关于无线网络隐私权保护的访问控制类研究主要是建立在有一家或多家授权认证机构的基础上，并且假定认证机构不可能被彻底破解。所以，有必要对无认证机构的访问控制机制进行深入的探讨。

（2）访问控制的设计可以在一定程度上阻止未经许可的使用者进入，但是一旦发生突发事件（例如患者的生命受到威胁），访问控制也会对其造成很大的影响。因此，将“突发事件处理”机制纳入到医学应用系统访问控制计划中，尚需深入探讨。

（3）随着多数据融合和大数据时代的到来，物联网作为互联网的扩展，其应用范围也日益扩大。许多物联网应用都需要提供实时的服务和快速的决策，而传统的密码算法和安全机制在物联网中不能满足需求。所以，有必要为实时业务设计一个轻量级的访问控制机制。

6 结语

总之，网络隐私权在当今世界日益受到人们的重视，每个公民都应该意识到自己的网络隐私的重要性，在理解网络隐私的基础上，更好地维护自己的个人和他人的网络隐私，使整个社会形成重视网络隐私的氛围，积极关注网络隐私立法趋势，了解网络隐私被侵犯时的维权手段。这将为网络社会构建一个更加纯粹、更加安全、更加和谐的网络空间。

参考文献：

[1] 张璐.无线网络中隐私保护的访问控制机制研究[D].曲阜师范大学,2020.

[2] 何道敬.无线网络安全的关键技术研究[D].浙江大学,2019.

[3] 唐阳雨.无线传感器网络访问控制研究[D].华南理工大学,2020.

[4] 苏铓.面向云计算的访问控制技术研究[D].西安电子科技大学,2019.