基于 JWT 的 EAST 实验数据用户身份和服务权限认证

申正阳[1,2] 王 枫[1] 任环宇[1,2]

[1](中国科学院合肥物质科学研究院等离子体物理研究所 安徽 合肥 230031)

[2](中国科学技术大学 安徽 合肥 230026)

摘 要 用户身份和服务权限认证已成为身份验证和数据访问安全的重要手段。用户身份认证采用动态令牌技术 JWT 实现。针对 JWT 丢失和被截获的问题,提出加密存储、解密使用的策略和 IP 与 JWT 绑定机制。根据 EAST 实验数据和用户的现状,将用户资源划分为二级用户,将服务资源划分为三级资源,采用图数据库 Neo4j 存储用户和资源之间的权限关系,并提出位图法加速权限认证。实验结果表明,基于 JWT 的认证方法及其安全策略能够有效解决身份和权限认证的问题。相较于传统的关系数据库存储用户权限,图数据库 Neo4j 和位图法能有效地提高权限认证效率。

关键词 身份认证 权限认 JWT EAST 图数据库 位图法

中图分类号 TP3 **文献标志码** A DOI:10.3969/j.issn.1000-386x.2024.05.047

JWT BASED USER IDENTITY AND SERVICE AUTHORITY AUTHENTICATION FOR EAST EXPERIMENTAL DATA

Shen Zhengyang[1,2] Wang Feng[1] Ren Huanyu[1,2]

[1](*Institute of Plasma Physics, Hefei Institutes of Physical Science, Chinese Academy of Sciences, Hefei 230031, Anhui, China*)

[2](*University of Science and Technology of China, Hefei 230026, Anhui, China*)

Abstract User identity and service authority authentication have become important means of identity verification and data access security. User identity authentication is implemented using dynamic token technology JWT. For the problems of JWT being lost and intercepted, the strategy of encrypted storage and decryption and the binding mechanism of IP and JWT are proposed. According to the EAST experimental data and the current status of users, user resources were divided into second-level users, and service resources were divided into third-level resources. Graph database Neo4j was used to store the authority relationship between users and resources, and a bitmap method was proposed to accelerate authority authentication. The experimental results show that the JWT based authentication method and its security strategy can effectively solve the problems of identity and permission authentication. Compared with the traditional relational database storing user permissions, the graph database Neo4j and the bitmap method can effectively improve the efficiency of authentication.

Keywords Identity authentication Authority authentication JWT EAST Graph database Bitmap

0 引 言

EAST (Experimental Advanced Superconducting Tokamak)是我国建造的国际上第一个全超导核聚变实验装置[1]。EAST 实验数据主要包括运行状态监控数据、工程诊断数据和视频数据等,分散地存储在各自的子系统中。运行状态监控数据是 EAST 各个装置的实时监控数据,如真空、低温、水冷、电源和技术诊断等装置。各个装置拥有独立存储系统和设备,采集的运

收稿日期:2021-01-30。国家磁约束核聚变能发展研究专项项目(2018YFE0302100)。**申正阳**,硕士生,主研领域:数据访问。**王枫**,副研究员。**任环宇**,硕士生。

行状态监控数据、用户数据主要存储在各自的 MySQL 数据库中。用户身份认证通过查询各个子系统的用户数据库表完成认证,并采用 Cookie/Session 的方式记录用户信息;当用户认证通过时,即拥有整个子系统及其数据的访问权限。工程诊断数据包括激光诊断、光谱诊断、微波诊断、电磁测量、高能粒子诊断、核测量等诊断数据,主要存储在 MDSplus(Model Drive System plus)数据库中[2-3]。目前,这部分数据的访问不需要任何的身份和权限认证。视频数据主要以视频文件的方式存储,采用 Cookie/Session 的身份认证方式,缺乏权限认证和管理。访问视频数据时,仅需要身份认证就能够访问所有视频数据。

现有的用户身份认证和服务权限认证主要通过各个分散的子系统进行认证,甚至访问工程诊断数据不需要任何的身份认证和权限认证。因此建立统一的身份认证和权限认证,有利于管理用户和分配用户权限,提高 EAST 实验数据的访问安全性。

针对 EAST 实验数据的存储分散、数据传输协议不统一等问题,基于动态令牌 JWT 的身份认证方法具有天然的去中心化、不依赖任何传输协议和浏览器等特点,有利于分散的子系统进行身份认证。另外 JWT 的 PayLoad 部分能够记录用户信息,方便用户信息的传递,以及支持多种加密方式提高了令牌签名的安全性。

虽然,动态令牌 JWT 身份认证机制具有去中心化、方便分布式权限认证、不用存储用户信息等优势,但也存在令牌丢失或被截取等安全问题。权限认证大都采用基于角色的访问方法。该方法通过角色来连接用户和权限之间的关系,简化了用户权限的分配。

本文基于动态令牌 JWT 技术实现了用户的身份认证;通过将用户 IP 地址与 JWT 绑定提高了令牌传输过程中的安全性;采用对称加密算法将令牌加密存储、解密使用,提高了令牌使用过程中的安全性。服务权限认证将用户划分为不同的组,从而形成用户级和用户组级的二级划分。根据 EAST 数据的存储现状,将服务资源划分为服务接口方法、数据源和数据的三级资源。因为同一用户组下的用户通常拥有相同的服务资源的访问权限,因此通过用户组关联相应接口方法、数据源等实现用户的权限分配。相较于使用关系数据库存储用户的权限信息,本文采用图数据库存储有效地提高了服务权限认证的效率。为进一步提高权限认证的速度,提出位图法来记录用户是否有相应服务或资源访问权限。

1 相关工作

传统的身份认证一般采用 Cookie/Session 身份认证机制[4]。该方法在客户端的 Cookie 中记录对应 Session 的 JSESSION_ID,在服务端维持包含用户信息的 Session。用户通过发送 Cookie 进行身份认证,服务端使用 Cookie 中的 JSESSION_ID 来验证对应 Session 中的用户信息。基于 Cookie/Session 的身份认证方法需要服务端在内存维持用户 Session 的状态,当用户达到一定规模时,会对服务端内存造成压力,另外 Cookie 需要浏览器支持和不具有跨域访问的特点。基于动态令牌的身份认证通常将用户的信息存储在令牌中,服务端不需要存储用户身份,这有利于分布式的服务权限认证[5-6]。具体来讲,服务端接收到用户的登录请求后,验证用户信息,若验证通过使用加密算法将用户信息加密成为令牌,并发送给客户端存储。当客户端调用服务时需携带该令牌发送请求,服务端通过验证令牌进行用户身份认证。目前,基于动态令牌的认证方法有 OAuth(Open Authorization)[7-8]、JWT(Json Web Token)[9]等。OAuth 通常使用第三方的用户信息登录系统,如微信、微博等的登录。OAuth 首先通过地址重定向跳转到第三方系统的登录界面,然后用户登录并授权,之后将返回一个授权码,接着通过授权码获取用户的令牌,最后使用令牌换取用户的信息。JWT 是令牌的一种具体形式,它主要包括三个部分:Header、Payload 和 Signature。Header 通常包括令牌的类型和使用的加密或散列算法。Payload 用来存放需要传递的数据,通常包括令牌的授权方、用户信息、令牌的有效时间等。Signature 表示前两部分的签名,通常使用加密算法加密生成。相较于 Session 中存储用户的身份,动态令牌将验证信息存放在令牌字符串中,简化了用户身份的认证,但也存在一定的安全问题。当令牌丢失或被截获时,获得令牌的人员可以访问令牌所拥有权限内的所有服务。针对该问题,文献[10]提出了一种多因子混合的签名策略;文献[11]提出了一种基于动态令牌的双向认证方案。本文通过将令牌与客户端 IP 绑定保障了传输过程中的安全性;通过将令牌加密存储和解密使用,保障了客户端在使用过程中的安全性。IP 绑定:当用户登录系统时,服务端生成动态令牌 JWT 并在其 Payload 中设置连接的 IP 地址实现 IP 绑定;当用户调用服务访问数据资源时,验证 JWT 中 IP 地址与客户端连接的 IP 是否一致,保障客户端的真实性。若 IP 不一致,则为伪造客户端。若 IP 验证一致,则验证 JWT,若 JWT 验证失败,则 JWT 中的 IP

被篡改。加密存储和解密使用:当客户端接收到 JWT 时,使用 SnowFlake 算法生成加密密钥,使用对称加密算法 AES 加密 JWT,然后存储加密后的 JWT;当使用 JWT 访问服务时,客户端通过使用密钥解密并携带 JWT 请求服务资源。

服务权限认证用于限制用户对资源的访问控制权限。自主访问控制(DAC)是直接赋予用户相应的资源访问权限[12]。但是,当用户数量和资源数量庞大时,采用 DAC 方式的授权操作将变得相当复杂,难以管理。强制访问控制(MAC)是系统要求用户和系统资源满足强制的访问控制策略[12]。但 MAC 偏向于系统的安全性,不适合授权管理。基于角色的访问(RBAC)就是用户通过角色与权限进行关联[13]。简单地说,一个用户拥有若干角色,每一个角色拥有若干权限。基于属性的访问控制(ABAC)将用户和资源特性抽象出属性特征,通过管理属性之间的关系进行访问权限的控制[14]。本文分析了用户和 EAST 实验数据的存储现状,进行二级用户和三级资源划分,通过用户组和资源以图方式关联起来,实现用户权限的管理。

2　用户身份认证

身份认证是验证用户信息,阻止非法用户访问系统资源的重要手段。基于动态令牌的认证方式有效克服了传统基于 Cookie/Session 的身份认证弊端。针对令牌传输过程中丢失和易被截获的问题,使用对称加密和 IP 绑定的方法保障令牌传输和使用过程中的安全。如图 1 所示,客户端首先根据用户名和密码登录;服务端验证通过后生成动态令牌 JWT 并在 Payload 中设置 IP 地址;客户端接收 JWT,使用 SnowFlake 算法生成加密密钥,使用对称加密算法 AES 加密 JWT,并存储加密后的 JWT;之后,客户端通过携带 JWT 请求服务资源;服务端验证 IP 地址的一致性,验证 JWT 的合法性,验证用户是否拥有服务权限,最后将请求的数据发送给客户端。

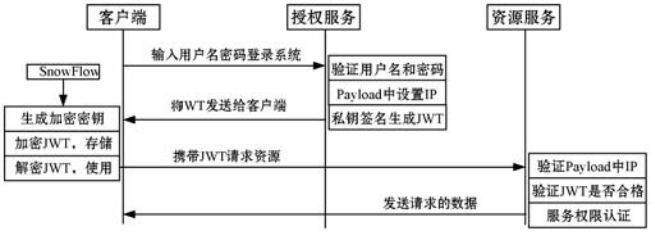

图 1　用户身份认证

2.1　IP 地址与 JWT 绑定

本文设计的 JWT 格式如图 2 所示。Header 部分记录了加密算法为 RSA 非对称算法,数据类型为 JWT。Payload 中主要存放了授权方、有效时间、用户信息、IP 地址等数据。Signature 表示 Header 和 Payload 两部分使用 RSA 签名后形成的字符串。当服务端生成 JWT 时,通过将 IP 地址记录在 Payload 中,实现 IP 与 JWT 的绑定。当服务端验证 JWT 时,验证 Payload 中 IP 地址与客户端连接的 IP 是否一致,保障客户端的真实性。若 IP 不一致,则为伪造客户端。若 IP 验证一致,则验证 JWT,若 JWT 验证失败,则 JWT 中的 IP 被篡改。

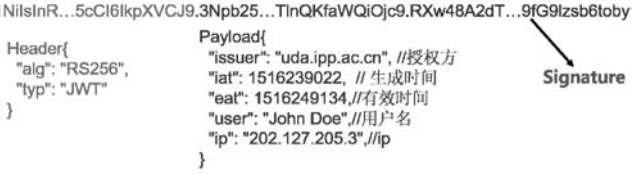

图 2　JWT 数据格式

2.2　JWT 的加密存储和解密使用

本文采用 AES 对称加密算法[15]加密 JWT。由于 AES 算法密钥长度需要 128 位,因此通过拼接 SnowFlake 算法产生的唯一 ID 和当前时间戳生成 128 位的 JWT 加密密钥。SnowFlake 算法结果是一个 64 位的长整型 ID,其中 41 位作为毫秒数,10 位作为机器号,12 位作为毫秒内的流水号,最后还有一个符号位,一般为 0。时间戳可转化为 64 位的长整型变量。当客户端在接收到 JWT 时,使用对称加密算法 AES 将 JWT 加密存储在本地,使用的时候通过 AES 算法和密钥解密 JWT。由于客户端在使用过程中存储的都是加密的 JWT,有效降低了 Token 被窃取的风险。

3　服务权限认证

本文根据 EAST 用户群体和实验数据存储的特点,进行了两级用户、三级资源划分。两级用户划分将用户划分到不同的群组,比如低温组、中心束注入组、聚变堆包层组、偏滤器组、控制与采集组等。两级用户分别为用户和用户组。三级资源分别为服务接口方法、数据源和数据。服务接口方法包括获取实验数据的方法、获取元数据的方法、获取权限管理数据的方法等。数据源主要包括各个系统运行状态监控数据如低温、真空、电源、水冷和技术诊断等状态监控数据源,工程诊断数据源如 EAST、PCS_EAST、PF_EAST 等,另外还有部分视频数据源。数据包括运行状态监控数据的数据库表、工程诊断信号名和视频监控数据的视频文件名。通过用户和用户组的关联将细粒度的用户转化

为了大粒度的用户组,方便了用户权限管理。三级资源的划分建立接口方法和资源之间的关系,方便了服务资源的管理。用户和服务资源之间通过图连接进行权限管理,并存储于图数据库 Neo4j 中,如图 3 所示。图 3 中表示用户“申正阳”所属的用户组为“控制与采集组”;“控制和采集组”拥有五个接口方法的权限;这五个方法关联着 MDSplus、MySQL、Neo4j 三个数据源;数据源又连接着用户能够访问的数据项。由于 EAST 实验数据存储和访问的复杂性,造成用户权限分配的困难,而采用图数据库设计和存储用户的权限不但降低了权限分配难度,并且加快了权限认证的效率。

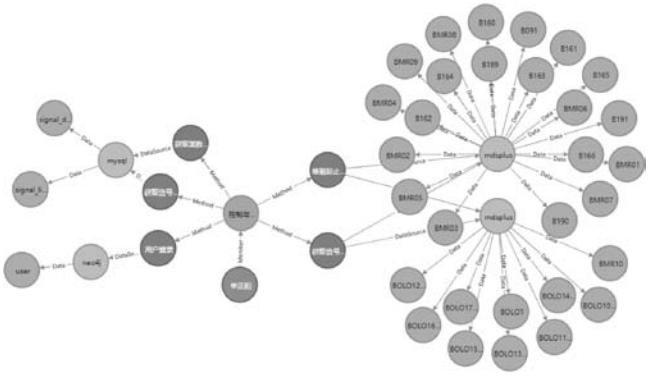

图 3 图数据库 Neo4j 存储用户权限

相较于传统的关系数据库,图数据库 Neo4j 采用图的形式存储权限的关系,有利于多层级的权限分配和管理,以图搜的方式查询用户权限,具有高效的权限查询效率。若采用关系数据库,则需要设计用户和资源实体表五项、连接表三项,造成权限设计和管理的复杂。图数据库 Neo4j 将用户和资源作为节点,将用户和资源、资源和资源之间的关系抽象为边,简化了 EAST 中的多层级资源之间的权限关联。图数据库 Neo4j 的权限管理仅需要将相应的节点进行添加和删除,权限管理方便。

使用位图法加速权限认证。位图法就是用每一位存放某种状态,这里表示是否有访问资源的权限。根据三级资源划分的结果设计了三个位图分别表示服务接口方法位图、数据源位图、数据位图。当用户调用某服务时,查询位图中对应的资源位是否为 1,若为 1 则执行相应的服务,为 0 则拒绝。若位图为空,则利用 JWT 中携带的用户信息查询权限数据库 Neo4j 中用户所用的权限信息,并将位图中能够访问的资源设置为 1,并在内存中初始化位图。

具体来讲,位图法将每一级的资源进行编号,如服务接口根据接口名进行编号;当用户调用服务时,从图数据库获取用户所拥有的资源权限,初始化位图并根据资源的编号将相应位置为 1。图 4 为服务接口方法位图,用户拥有的接口方法有获取信号、获取信号属性、获取分段信号、用户登录等方法,对应的编号分别为 1、3、8、12,当服务接口方法位图初始化时分别将第 1、3、8、12 位设置为 1,表示用户拥有该方法资源权限。

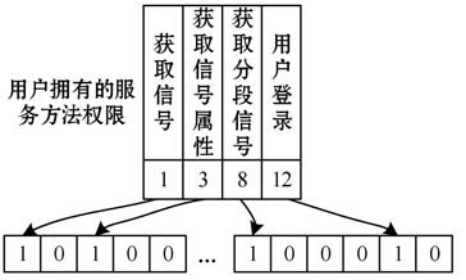

图 4 服务接口方法位图

服务方法和数据源的位图使用 char[1 024]记录,1 024 个 char 类型的数据可以记录 8 000 个资源。由于仅 EAST 中工程诊断信号就包含 7 000 多个信号,数据项比较多,因此使用 char[10 * 1 024]记录数据位图。

4 系统实现和实验结果

4.1 用户和权限管理系统

权限管理系统界面采用 Vue[16] 前端框架开发,主要包括的功能有用户的管理、服务资源的管理和用户和服务之间的关联。图 5 表示用户管理包括用户列表和用户组列表,能够添加用户、查询用户、修改用户信息、删除用户等。图 6 表示服务资源管理主要包括服务接口方法、数据源、数据项等的管理。图 7 表示用户组的权限管理,通过添加、删除、修改用户组和服务资源之间的关联实现。

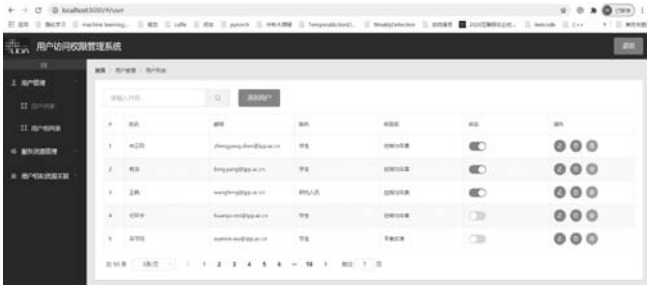

图 5 用户管理

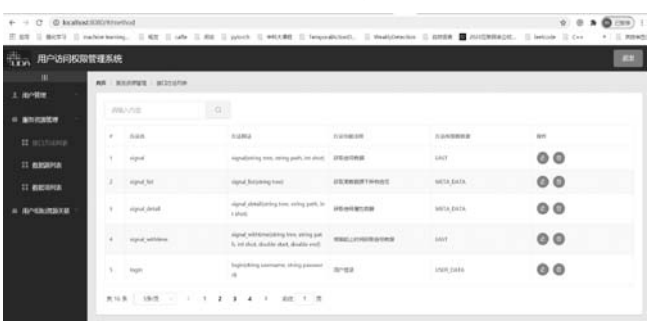

图 6 服务资源管理

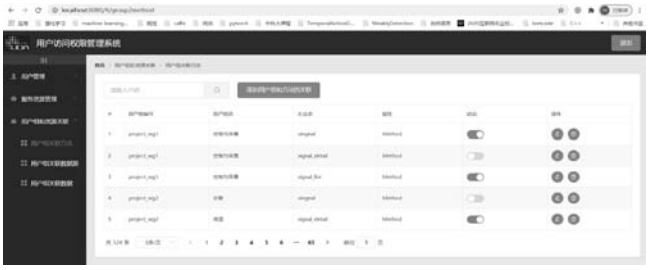

图 7　用户组和服务资源之间的关联

4.2　身份和权限认证测试结果

EAST 实验数据访问主要包括客户端库和 C ++ 后台服务两个部分。本文通过使用客户端库调取后台服务的方式来验证用户身份认证和服务权限认证。

身份认证主要包括用户认证、IP 认证和 JWT 认证。当用户登录时,进行用户认证,服务端验证其用户名和密码的正确性;当用户调用服务时,进行 IP 认证和 JWT 认证,验证其 IP 地址和 JWT 令牌的正确性。如图 8 所示,当上述身份认证任何一个失败时,后台服务会设置错误码,客户端根据错误码提示 login failed 异常,例如"login failed by ip exception"。

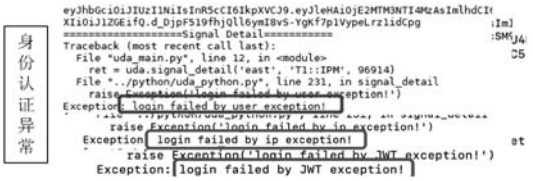

图 8　三种身份认证异常

权限认证主要验证用户所拥有的资源是否满足用户所调服务的需求,若不满足则提示"access permission exception"异常。如图 9 所示,当访问获取 T1:IPM 信号服务时,系统会从图数据中查询用户权限并更新位图,若用户数据位图中信号 T1:IPM 为 0,则没有访问权限,则会提示异常,例如"access data T1:IPM permission exception"。

图 9　权限认证异常

当用户调用服务时,分别进行上述的身份认证和权限认证,若认证通过,服务端返回 JWT 和相应的数据,如图 10 所示。

图 10　正确调用服务

4.3　权限认证时间比较

图 11 展示了查询用户权限的时间比较,横轴表示用户的数量,纵轴表示用户验证权限的相应时间。实验的环境是:CPU 型号为 Intel(R) Xeon(R) CPU E5-2640 v3 @ 2.60 GHz,CPU 数量 1,CPU 核心数为 8,内存 64 GB。从图 9 可以看出 Neo4j 的用户权限的查询时间明显低于 MySQL。

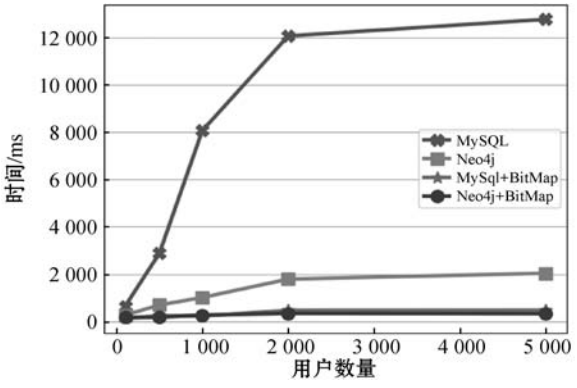

图 11　数据库权限认证查询时间比较

由于用户和资源的复杂性,导致传统关系数据库的表设计繁杂,用户和资源实体表有五项,连接表有三项。每次用户查询需要这 8 个表进行 Join 操作,而关系数据库的 Join 操作是低效的,这造成查询响应时间较长。图数据库没有表结构,避免了表之间的 Join 操作,而是通过图连接查询用户拥有的权限资源。从图 11 中还可以看出使用位图法查询时间明显变短。这是因为位图直接将用户的权限存放到内存中,避免了数据库的查询,加快了用户权限的验证过程。

5　结　语

本文根据用户的现状,基于 JWT 技术构建了用户身份认证系统,针对令牌丢失的问题提出 IP 绑定和加密存储的安全策略。通过分析 EAST 数据存储的现状,将用户和资源划分为二级用户和三级资源,基于图数据库 Neo4j 以图的方式构建用户和资源之间的访问权限。为进一步加快权限认证的过程,提出位图法。实验结果表明,系统能够管理用户、服务资源,能够正确进行用户权限认证和服务权限认证,以 Neo4j 存储用户权限能够较大程度提高权限认证的效率。下一步将继续研究位图法在权限认证中的高效刷新机制。

参　考　文　献

[1] 万宝年,徐国盛. EAST 超导托卡马克[J]. 科学通报,2015,60(23):2157 - 2168.

[2] 林冬涛,肖炳甲,袁旗平. MDSplus 数据存储应用[J]. 微计算机信息,2010,26(34):111 - 113.

(下转第 344 页)

其最小值为0.5,通常用一个 AUC 大于 0.5 的多少来衡量其比链路预测其比随机相似度算法好的程度[17]。通过表3 可以看到这三个数值均大于 0.5,因此实验能够预测到那些随机删除或未来可能存在的连边,且比随机相似度算法好。

表 3 链接预测的曲线下面积(AUC)评分

数据集	杰卡德系数	Adamic-Adar 指数	优先链接
《水浒传》	0.524 1	0.521 9	0.518 8

3 结 语

阅读文学作品可以培养人们的文学素养,其一般都反映了当时的社会背景,因此理清人物之间的关系对文学作品的分析以及正确理解文章很重要,然而人们往往是通过阅读全文的方式,获得人物关系以及对文章的理解,但这样得到的结果有很大一部个人主观因素影响,不同的人可能对同一篇文章有不同的理解。本文使用复杂网络的方法,搜索获得人物名称文件,代码得到人物之间关系的连边文件,以任意两个人物在不同章回的共现次数作为权重,构建无向加权网络,对文学作品进行了客观分析,实现了《水浒传》的一百单八将人物关系网络的可视化,在实验部分计算了人物关系网络的度、网络直径、平均路径长度、介数、集聚系数,模块度以及链接预测分析了《水浒传》的人物关系网络,最后发现其具有小世界网络特性以及社区特性。

参 考 文 献

[1] 吉红宇. 基于复杂网络分析的人物关系挖掘[D]. 成都:电子科技大学,2017.

[2] 张荣杰. 感知与现实人际关系网络:经典文学作品分析[D]. 漳州:闽南师范大学,2018.

[3] 陈蕾,胡亦旻,艾苇,等. 红楼梦中社会权势关系的提取及网络构建[J]. 中文信息学报,2015,29(5):185 - 203.

[4] 赵京胜,张丽,朱巧明,等. 中文文学作品中的社会网络抽取与分析[J]. 中文信息学报,2017,31(2):99 - 106,116.

[5] 董晓烨,柴静. 语料库辅助的文学作品主题分析[J]. 西安电子科技大学学报(社会科学版),2018,28(3):106 - 111.

[6] 楼锴毅,霸元婕,李绍昂. 基于社交网络的小说聚类[J]. 软件工程,2018,21(10):14 - 16.

[7] 涂轶文. 基于人物相似度的互联网络人物关系分析方法研究[D]. 成都:电子科技大学,2019.

[8] 林峰,赵广平,林娜,等.《红楼梦》文本的社会网络结构分析[J]. 石家庄铁道大学学报(社会科学版),2018,12(1):58 - 63.

[9] 唐毅,王硕,胡桓.《水浒传》人物关系网络的文本挖掘[J]. 社科纵横,2018,33(4):117 - 120.

[10] 李娇. 基于共现与关联挖掘的人物关系图谱研究与实现[D]. 兰州:西北民族大学,2019.

[11] 胡岚曦. 一种基于行为分析的人物关系网络发掘方法[J]. 计算机应用与软件,2009,26(10):256 - 258.

[12] 任东升,马婷. 基于语料库的《水浒传》沙博理英译本意合句式研究[J]. 外语研究,2015,149(1):64 - 70.

[13] 杜贵晨.《水浒传》茶事考论[J]. 陕西理工学院学报(社会科学版),2016,3(4):1 - 10.

[14] 李桂奎. 论《水浒传》"怒气"摹写之"乖错"情理[J]. 中原文化研究,2020,8(3):92 - 100.

[15] 李泽荃,杨嶷,刘嵘,等. 复杂网络与机器学习融合的研究进展[J]. 计算机应用与软件,2019,36(4):11 - 28,62.

[16] 熊中敏,朱春卫,郭振辉,等. 基于 OLAP 和聚类分析的关联规则挖掘方法[J]. 计算机应用与软件,2018,35(5):58 - 61.

[17] 司帅宗. 社会网络中的链路预测及网络重构[D]. 沈阳:东北大学,2014.

(上接第 331 页)

[3] Stillerman J, Fredian T, Klare K, et al. MDSplus data acquisition system[J]. Review of Scientific Instruments,1997,68(1):939 - 942.

[4] Choi Y, Loo Y, LaCroix K. Cookies and sessions: A study of what they are, how they can be stolen and a discussion on security[J]. International Journal of Advanced Computer Science and Applications,2019,10(1):32 - 36.

[5] 李慧琴. 基于动态令牌的网关服务访问认证的研究与实现[D]. 郑州:河南大学,2020.

[6] 黄伟民,陈可新. 基于 Token 的物联网云平台系统身份认证机制研究[J]. 智库时代,2018(42):195 - 196.

[7] 汪昱. 应用程序认证机制安全研究[D]. 西安:西安电子科技大学,2018.

[8] Jones M, Hardt D. The OAuth 2.0 Authorization Framework: Bearer Token Usage[EB/OL]. (2020 - 03 - 07). https://tools. ietf. org/html/rfc6750.

[9] Jones M. JSON Web Token[EB/OL]. (2020 - 03 - 07). https://tools. ietf. org/html/rfc7519#section-10. 2. 1.

[10] 程治胜. 一种多因子策略混合 Token 签名算法[J]. 电子技术与软件工程,2019(5):149.

[11] 顾洁. 面向无线社区的身份认证及密钥管理技术研究[D]. 上海:上海交通大学,2012.

[12] 陈晓. 电力企业信息系统中统一身份认证与访问控制应用研究[D]. 北京:华北电力大学,2013.

[13] 李春燕. 云计算环境下基于角色的访问控制模型研究[D]. 天津:天津大学,2012.

[14] 何修宇. 微服务环境下访问控制技术的研究与应用[D]. 北京:北京邮电大学,2018.

[15] 樊昊鹏,袁庆军,王向宇,等. 针对 AES-128 算法的密钥优势模板攻击[J]. 电子学报,2020,48(10):2003 - 2008.

[16] Lopez D. Full-Stack web development with Jakarta EE and Vue. js[M]. Apress Berkeley,2021.