**Operations Research and Fuzziology** 运筹与模糊学, 2023, 13(4), 3369-3378
Published Online August 2023 in Hans. https://www.hanspub.org/journal/orf
https://doi.org/10.12677/orf.2023.134340

Hans汉斯

# 政府数据安全治理研究：热点主题与演化趋势

**卢春芸**

贵州大学公共管理学院，贵州 贵阳

收稿日期：2023年6月15日；录用日期：2023年8月5日；发布日期：2023年8月10日

## 摘　要

**基于CiteSpace软件及WoS核心数据合集，对2008~2022年发表的政府数据安全治理相关研究进行文献计量统计及可视化分析，探讨近15年来该领域的研究热点主题和发展演化趋势。结果显示，在有效的665篇文献可视化分析中，政府数据安全治理研究包含了数据安全政策、物联网、数字水印、区块链、深度学习、数据泄露、数据共享等热点主题，再结合可视化分析结果以及文献的阅读，将政府数据安全的治理归纳为两个方面，即“技术 + 政策”，为该领域未来研究提供一些思路和参考。**

## 关键词

**政府数据安全，可视化分析，CiteSpace，Web of Science**

# Research on Government Data Security Governance: Hot Theme and Evolutionary Trend

**Chunyun Lu**

School of Public Administration, Guizhou University, Guiyang Guizhou

Received: Jun. 15th, 2023; accepted: Aug. 5th, 2023; published: Aug. 10th, 2023

## Abstract

**Based on CiteSpace and Web of Science (WoS) core data collection, the article conducts bibliometric statistics and visual analysis of the government data security governance published in 2008~2022, and discusses the hot topics and evolution trends in this field in the past 15 years. The results show that in the effective 665 literature visualization analysis, the government data security governance research contains data security policy, Internet of things, digital watermarking, block chain, deep learning, data leakage, data sharing, etc. Combined with visual analysis results and li-**

文章引用: 卢春芸. 政府数据安全治理研究: 热点主题与演化趋势[J]. 运筹与模糊学, 2023, 13(4): 3369-3378.
DOI: 10.12677/orf.2023.134340

**terature secondary reading, the government data security management can be classified into two aspects, namely "technology + policy". This research provides some ideas and references for future research in the field.**

## Keywords

**Government Data Security, Visual Analysis, CiteSpace, Web of Science**



## 1. 引言

数据安全是数字政府的生命线，近年来，智能系统面临对抗性样本、数据污染、数据泄露等数据安全威胁，导致严重的智能系统安全隐患[1]。尤其是物联网与人工智能的结合更是加大了具有跨领域、跨部门、多元异构等特征[2]的政府数据安全及风险问题，给各国经济发展和社会稳定带来严重威胁，政府数据安全治理工作成为政府和社会亟待解决的问题。与此同时，学术界积极对相关问题进行研究并从不同角度对政府数据安全的治理工作进行探讨。张涛基于区块链并从可追溯机制、防篡改机制及共监管机制三个方面探讨政府数据安全治理的机制变革[3]；黄璜将其分为宏观、中观和微观三个层面并从中观层面，即政府对在社会公共事务治理中所产生或需要的数据资源的治理，涉及政府数据资源的利用、共享和开放等核心议题[4]；美国、英国、澳大利亚等发达国家(地区)从政策法规、组织架构、数据平台等方面设计并实施政府数据治理体系，以推动数据利用为重要目标[5]。在作用和意义上，政府数据安全可以防止财产欺诈[6]、在社区内建立信任、增强社区参与感、增强公民能力等。面对复杂的政府数据安全治理研究主题，有必要对其进行全面的文献梳理。

基于此，本文利用 WoS 核心合集数据库，采用 CiteSpace 知识图谱和文献计量法，从文献发文量、研究力量、关键词等多维度回顾总结和分析当前国际政府数据安全治理研究成果和发展动态。

## 2. 数据来源与分析方法

### 2.1. 数据来源

文本数据来源于 WoS (Web of science)核心数据库，将索引限定为 SSCI (Social Sciences Citation Index)和 SCI-Expanded (Science Citation Index Expanded)文献，保证了所收集数据的权威性和说服力，文献类型精炼为期刊论文(Article)，以广泛意义上与“政府数据安全”关联密切的英文表达式作为主题检索词，检索式为 TS = (governmental OR government OR administration OR State) AND TS = (“data safety” OR “information-safety” OR “statistics safety” OR “datasecurity” OR “information security” OR “statisticssecurity” OR “data risk” OR “information risk” OR “statistics risk”)，检索时间不设限制，但因为有关论文于 2008 年才首次出现，所以时间跨度为 2008~2022 年(具体检索日期为 2022 年 11 月 2 日)。为了保证数据的准确性，通过人工对文献进行筛选，将与研究主题不相关的文献剔除，再通过 CiteSpace 进行去重，最终得到有效文献 665 篇。

### 2.2. 分析方法

本文先采用 EXCEL 对发文量及普莱斯曲线进行统计分析，再借助 CiteSpace 6.2.R4 可视化软件进行

数据处理，对该领域发文作者、机构、国家、关键词进行分析，得出相关知识图谱。通过文献计量工具，探寻出某特定领域演化的关键路径及知识转折点，最终以可视化图谱直观地呈现出来，增强人们对这些抽象信息的认知[7]。CiteSpace 绘制的图谱主要以节点(Nodes)和连线(Links)两种要素来表示，频次越高说明节点越大。

## 3. 实证分析

### 3.1. 文献发文量及查全检验

文献发表的数量及时间分布在一定程度上反映了这个领域的发展变化过程和学术界的关注程度。WoS 数据库中政府数据安全治理研究的文献发表年份分布图(如图 1)，可看出，文献数量总体上呈现波动增长态势，尤其是 2014 年以后增幅更为明显。这种情况说明政府数据安全治理研究越来越受到学术界的关注，研究热度在不断增强。本文尝试将其分为三个阶段进行分析：第一阶段为起步期(2008~2013 年)，仅发文 63 篇，仅占近 15 年总量的 9.5%，该阶段尚未引起学术界的广泛关注；第二阶段为突破发展期(2014~2017 年)，该阶段发文量较第一阶段有较大的提升，共发文 102 篇，占比 15.3%；第三阶段为蓬勃发展期(2018~2022 年)，共发文 500 篇，占发文总量的 75.2%，成果产量最多，是上一阶段的 5 倍。

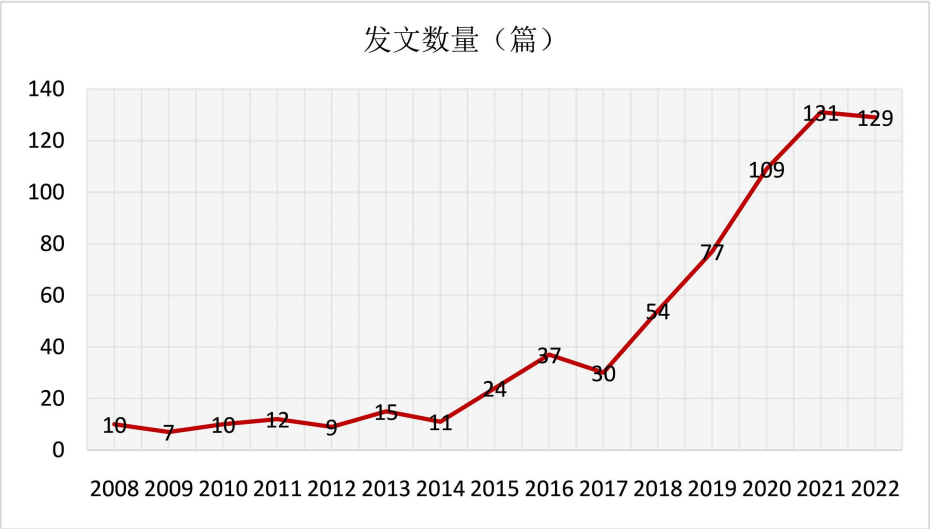


**Figure 1.** Annual volume of literature publications from 2008 to 2022
**图 1.** 2008~2022 年文献年度发文量

陈超美教授认为，在搜索文献资料时，应该着重于保证数据的查全率，通过普莱斯曲线(Price's curve)函数[8]进行验证。普莱斯曲线的数学表达式为：$F(t)=a\times e^{bt}$ $(a>0, b>0)$，其中 $F(t)$表示文献量，$a$ 为初始时刻文献发表量，即 2008 年的文献数量：$a=10$，e 为自然对数底，$b$ 是期刊的持续增长率，是一个时间常数。根据相关公式 $b=\sqrt[n]{A/a}-1$，其中 $n$ 为统计文献的时间年限，即 2008~2022 年之间的年份，$n=15$；$A$ 为发表文献累积数量，即 $A=665$，求得 $b=0.323$。最终得到 $F(t)=10e^{0.323t}$ ($t=$ 发文年份 $-2008$)，将所得的最终公式与实际文献累计量在图中拟合[9] (如图 2)。可得，本领域研究在出现和发展过程中的实际累计发文量和时间关系与普莱斯曲线拟合较好，说明本文在检索策略选择上比较合理，能够保证文献数据的查全率[10]。此外，根据该函数的短期预测功能，图 2 反映出政府数据安全治理研究在 2016 年后远未达到饱和状态，未来还有较大的发展空间[11]。

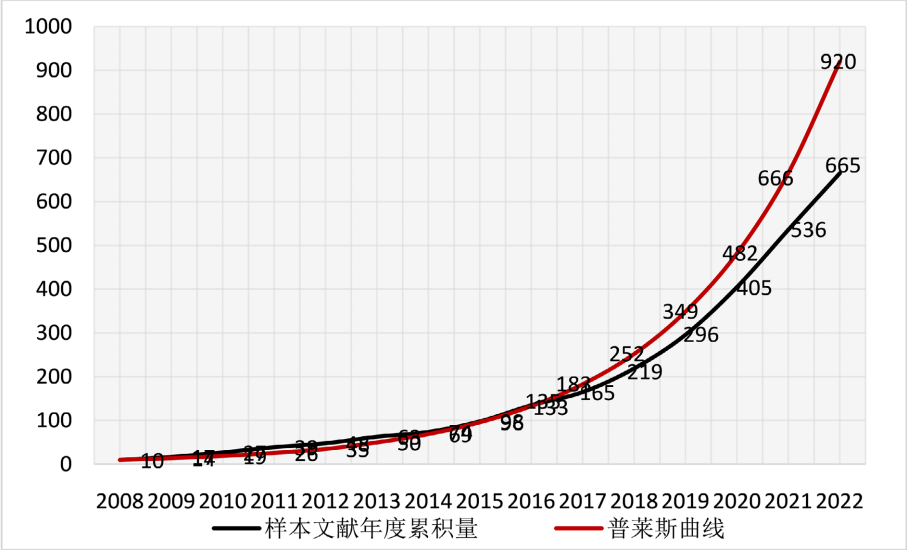


**Figure 2.** Annual cumulative number of literature and its Price curve for 2008~2022
**图 2.** 2008~2022 年文献年度累积数量及其普莱斯曲线

## 3.2. 研究力量分析

### 3.2.1. 核心作者的引领作用及合作分析

发文作者共现图谱能够识别出一个学科或领域的核心作者及其之间的合作强度和互引关系[12]。而核心作者代表着该研究领域的中坚力量，具有引领作用。根据上述操作步骤，绘制 WOS 核心引文数据库中政府数据安全治理研究发文作者共现图谱。其中，$N$ = 380 (节点)，$E$ = 219 (连线)，Density = 0.0026 (网络密度)，这说明有关政府数据安全治理研究数量不少，但合作的程度并不高。

根据普莱斯定律及其公式，$m = 0.749 \times (\eta\max)1/2$，可以判定出这一领域核心作者的范围。其中，m 代表核心作者发表论文的最小数量，ηmax 代表发表论文最多的作者的发文数量。根据图谱可知发文最多的作者为 Li X，共发文 9 篇，将 ηmax = 9 带入公式得到 $m$ = 2.25，因为论文数量需要取整数，所以 $m$ = 3，即表示发文量在 3 篇及以上的作者即为这个领域的核心作者。根据图谱信息可得核心作者共有 29 位，共发文 115 篇，占总发文量的 17.3%，分别是 Li X (9 篇)、KHAN M (8 篇)、WANG Y (6 篇)、LIU Y (5 篇)、WU Y (5 篇)等作者。从合作网络来看，以 LI X 为代表的团队规模最大，共有 8 人，除核心作者群体外，还存在着数量众多的独立作者群体，且其群体间的合作关系相对松散。

### 3.2.2. 作者所属机构分析

利用 CiteSpace 软件的 Institution 模块，对发文机构进行可视化，获取政府数据安全治理的机构合作关系图，并对其发文量和合作关系进行分析。其中，发文量最多的是 Tsinghua University (清华大学)，共发文 10 篇；其次是 Wuhan University (武汉大学)，共发文 8 篇，除此以外，发文量较多的机构还有 Xidian University (西安电子科技大学)、Sungkyunkwan University (成均馆大学)、Chinese Acad Sci (中国科学院)、Xi’an Jiaotong University (西安交通大学)、Beijing University of Posts & Telecommunications (北京邮电大学)、Duke University (杜克大学)、Nanjing University of Information Science & Technology (南京信息科技大学)、Korea University (高丽大学)等，从排名前十的机构可以看出研究机构均为学术研究综合性较强且影响力较大的高校研究机构，且中国的院校占比一半以上，这表明了中国学术界对政府数据安全治理的高度重视。此外，少数机构之间已存在合作关系，其中以成均馆大学为主的合作团队规模最大，已形成 9 个机构之间的合作。但仍然还有很多机构之间是独立研究。

### 3.2.3. 作者所在国家/地区分析

发文国家/地区能更好地了解政府数据安全治理的空间分布和世界各国的研究成果。通过 CiteSpace 软件 Country 模块对发文国家/地区进行可视化，得到政府数据安全治理研究国家/地区间合作关系图谱，进一步对其发文量及合作关系进行分析。其中，$N$ = 81 (节点)，$E$ = 159 (连线)，Density = 0.0491 (网络密度)，表明在政府数据安全治理研究领域的国家研究数量不少，且国家/地区之间存在着合作关系。其中，发文量最多的为中国，共发文 187 篇，其次是美国(149 篇)。发文数量较多的国家/地区分别还有印度(65 篇)、英格兰(58 篇)、韩国(43 篇)、澳大利亚(41 篇)、沙特阿拉伯(35 篇)、中国台湾(34 篇)、德国(25 篇)、巴基斯坦(23 篇)等。从图谱中可知，发文数量较多的国家已形成较强的合作关系。通过总结发现，总体上政府数据安全治理研究中发达国家的发文量偏多一些，发展中国家偏少一些，但是越来越多的发展中国家也在逐渐重视政府数据安全治理研究，尤其是中国和印度，发文数量排在前三。

## 3.3. 关键词分析

### 3.3.1. 关键词词频分析

关键词通常是文章研究思想中核心内容的浓缩与提炼，在某种意义上，高频关键词在一定程度上反映出该领域的研究热点。通过 CiteSpace 软件 Keyword 模块对关键词进行可视化，裁剪方式为最小生成树(Minimum spanning tree)，生成了政府数据安全治理研究关键词共现图谱(如图 3)及关键词聚类图谱(如图 4)，进一步对该领域研究热点主题进行分析。

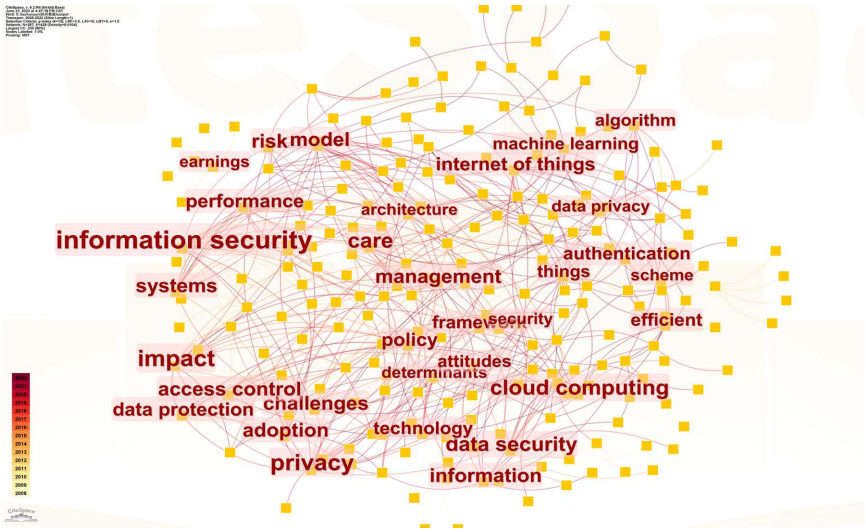


**Figure 3.** Keywords co-occurrence diagram
**图 3.** 关键词共现图

首先对相同意义的两个关键词(information security 和 data security)进行合并，通过数据整合最终得出 2008~2022 年间政府数据安全治理研究词频前 30 位关键词，如表 1，前 30 位关键词词频均在 12 以上，其中词频最高的关键词是“data security (数据安全)”，词频为 190；其次是“体系(system)”，词频为 51。从中心度来看，中介中心性起着连接各个节点的重要枢纽，中心度 > 0.1 的节点被定义为核心节点。由表可知中心度 > 0.1 的关键词分别有：数据安全(information security, 0.47)、体系(system, 0.12)、模式(model, 0.11)、影响(impact, 0.14)、访问控制(access control, 0.13)、采用(adoption, 0.11)。另外，数据安全、体系、模式的频次和中心度均排在关键词的前十位，说明数据安全问题、体系和模式受到研究者们的高度关注，是近 15 年来的研究热点。

**Table 1.** Frequency and centrality chart of government data security governance research hotspot from 2008~2022
**表 1.** 2008~2022 年政府数据安全治理研究热点关键词词频及中心度

| 序号 | 关键词 | 频次 | 中心度 | 序号 | 关键词 | 频次 | 中心度 |
|---|---|---|---|---|---|---|---|
| 1 | data security | 190 | 0.47 | 16 | Internet of thing | 20 | 0.02 |
| 2 | system | 51 | 0.12 | 17 | Access control | 19 | 0.13 |
| 3 | model | 45 | 0.11 | 18 | technology | 1 9 | 0.05 |
| 4 | management | 44 | 0.06 | 19 | thing | 1 8 | 0.04 |
| 5 | internet | 44 | 0.03 | 20 | network | 18 | 0.03 |
| 6 | framework | 34 | 0.10 | 21 | risk | 17 | 0.07 |
| 7 | Cloud computing | 33 | 0.08 | 22 | policy | 16 | 0.07 |
| 8 | scheme | 30 | 0.04 | 23 | adoption | 15 | 0.11 |
| 9 | challenge | 28 | 0.08 | 24 | Machine learning | 14 | 0.05 |
| 10 | security | 27 | 0.04 | 25 | effcient | 14 | 0.02 |
| 11 | privacy | 26 | 0.10 | 26 | design | 13 | 0.00 |
| 12 | information | 25 | 0.10 | 27 | performance | 13 | 0.04 |
| 13 | impact | 25 | 0.14 | 28 | Cyber security | 13 | 0.04 |
| 14 | Big data | 24 | 0.04 | 29 | Data protection | 12 | 0.05 |
| 15 | algorithm | 22 | 0.05 | 30 | Data privacy | 12 | 0.05 |

### 3.3.2. 关键词聚类分析

聚类是采用量化的方式计算，将内容中存在相似联系的词进行归纳，从而得到具有代表性的知识子群[13]。CiteSpace 依据网络结构和聚类的清晰度，通过 Q 值(模块值)和 S 值(平均轮廓值)两个指标来衡量图谱绘制的效果。

根据关键词信息，通过 LLR 算法对其进行聚类，得到 11 个主要的关键词聚类群，每个聚类群显性化地展示了政府数据安全治理研究领域中的一个前沿话题(如图 4)，其中 Q 值为 0.6513 > 0.3，S 值为 0.873 > 0.5，表明在政府数据安全治理研究中社会结构显著，聚类效果良好且聚类结果令人信服，有助于我们分析政府数据安全治理研究的总体特征和发展趋势。聚类图谱将现有的研究分为 11 个关键词聚类群，分别是#0 搭便车(free friding)、#1 物联网(internet of things)、#2 机器学习(machine learning)、#3 数据安全(information security)、#4 无线通讯 wireless communication)、#5 大数据(big data)、#6 移动计算(mobile computing)、#7 合规(compliance)、#8 数据安全(data security)、#9 数字水印(digital watermarking)、#10 医疗服务(medical services)。

### 3.3.3. 关键词突现分析

关键词是研究精华的体现，可以预测该学科领域的研究前沿，相对于单纯的高频关键词，突现词更适合探测学科发展的新兴趋势和研究转向。在关键词共现图谱的基础上，选择突现(Burstness)，将参数 $\gamma$ 调整为 0.8，得出 2008~2022 年政府数据安全治理研究关键词突现图谱(如图 5)，其呈现了政府数据安全治理研究的 9 个突现关键词(Keywords)及其突现强度(Strength)、突现时间(Year)、开始时间(Begin)和结束时间(End)。

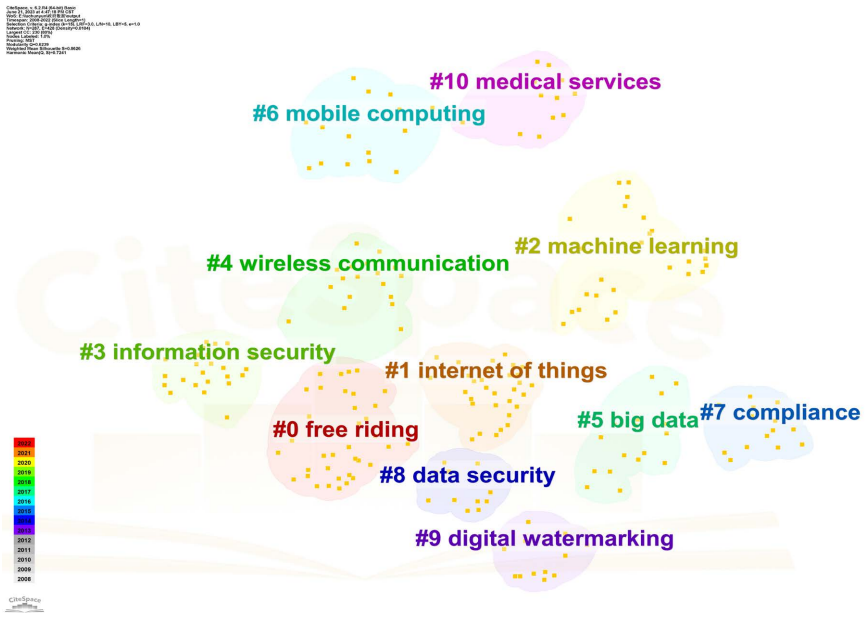


**Figure 4.** Keywords clustering graph
**图 4.** 关键词聚类图

**Top 9 Keywords with the Strongest Citation Bursts**

| Keywords | Year | Strength | Begin | End | 2008 - 2022 |
|---|---|---|---|---|---|
| computer security | 2008 | 2.61 | 2012 | 2017 | |
| deterrence | 2008 | 2.73 | 2013 | 2018 | |
| impact | 2008 | 3.33 | 2015 | 2017 | |
| privacy | 2008 | 2.35 | 2015 | 2018 | |
| risk | 2008 | 2.7 | 2016 | 2018 | |
| determinant | 2008 | 2.85 | 2018 | 2019 | |
| internet of things (iot) | 2008 | 3.18 | 2020 | 2022 | |
| thing | 2008 | 2.24 | 2020 | 2022 | |
| privacy protection | 2008 | 2.22 | 2020 | 2022 | |

**Figure 5.** Keywords emergence diagram of government data security governance in 2008~2022
**图 5.** 2008~2022 年政府数据安全治理研究关键词突现图

根据突现强度来看，政府数据安全治理研究中出现的关键词有 computer security (计算机安全)、deterrence (威慑)、impact (影响)、privacy (隐私)、risk (风险)、IoT (物联网)等，突现强度均在 2.22 以上。从突现时间来看，突现关键词也在不断地发生变化，可以看出“computer security (计算机安全)”、“deterrence (威慑)”两个词突现时间最久，时长为 6 年，对应的突现时间段分别为 2012~2017 年、2013~2018 年。同时，“privacy (隐私)”突现时长为 4 年(2015~2018 年)。根据高频关键词及突现时间，尝试将其分为三个阶段：

第一阶段为 2008~2015 年，计算机安全、云计算、数据保护、网络安全、制度等为该研究领域的热点关键词。这一时期更多注重技术设施安全、数据输入、数据输出、数据存储、数据处理等方面的安全

问题。自 2009 年开始，“大数据”成为互联网信息技术行业的流行词语，尤其 2012~2013 年间，大数据行业受到极大的关注，但由于技术相对不成熟，导致大数据技术落地艰难。而政府数据安全作为国家数据安全的重要组成部分，关系着国家安全与社会安全。同时，云环境中的政府数据面临诸如数据隐私侵犯、数据管辖权[14]等困境，给大数据时代的隐私和安全带来了巨大的挑战和风险[15]，再加上大数据的大容量、大速度、大品种和大真实性[16]增加了新的隐私和安全风险。为了部署云模型，Mircea 指出，有必要执行业务分析以有效地管理云计算数据安全[17]，组织必须确保数据被聚合或匿名化，以防止在大数据的快速传输、创建和处理过程中对个人身份信息集进行任何未经授权的访问。

第二阶段为 2016~2019 年，数据隐私、风险、挑战、互联网、机器学习等成为该研究领域的研究热点，这一时期，政府数据安全治理研究得到较快发展。自美国联邦政府于 2009 年颁布了《开放政府指令》以来，揭开了全球开放政府数据的序幕，随后，英国、加拿大等国家也纷纷出台了自己的数据开放条例。就中国而言，2015 年后，国务院提出加快政府数据开放平台的建设，按照规范数据格式对社会开放政府数据，到 2017 年数据开放平台开始呈现爆发式增长。然而，数据开放共享过程中带来的诸如质量管理差、安全管控弱、开放共享难等[18]数据安全和风险问题，引起学界和社会的广泛关注，人们逐渐重视隐私保护，数据治理也成为政府治理的重点领域和重要方式。此外，这时期的研究还初步尝试融入区块链技术提高数据安全性和隐私保护。2016 年 12 月，贵阳市在全国范围率先提出将区块链技术应用于政务中，引入区块链技术推动精准扶贫[19]。蒋余浩等提出大数据决策已引发多种决策风险，传统的公共决策责任机制难以有效应对，而应用区块链技术可以在一定程度上克服大数据崛起所带来的不确定性和碎片化等风险[20]。

第三阶段为 2020~2022 年，相关研究主要围绕物联网、隐私保护、效率、服务、体制方案等主题展开。从国内外研究现状来看，基于区块链的物联网技术已经得到广泛应用。物联网(IoT)一词自 1999 年由英国技术先驱凯文·阿什顿(Kevin Ashton) [21]创造以来，被不断扩展和深化，它是指日常设备连接到互联网，生成有关我们和我们周围世界的数据[22]，是推进“信息化”到“智能化”的关键手段，其与云计算带来的全球新概念、新技术的快速发展和深度应用与合作使得各行各业逐渐走向“智能”现代社会。龚惠群等通过文献计量和专利分析相结合的方式对全球物联网进行研究，得出国外对物联网的研究主要集中在终端设备、控制系统等基础设施和理论角度方面，而国内更侧重于技术和应用角度，包括云计算、ZigBee、智慧城市等[23]方面的研究。然而，新兴的物联网制度和智能应用的快速发展在消费电子环境网络中产生了许多新的无线安全漏洞，物联网会产生信息被滥用的风险，对遍布全球的物联网装置生成的大量数据造成了威胁。针对目前物联网应用中面临的安全威胁问题，近些年许多学者如 Piao CH [24]、Tan Evrim [25]、Haining Luo [26]等将区块链技术融入到物联网中，构建诸如链上服务方法、深度学习网络、防火墙安全技术等以实现物联网的安全性，它可以解决阻碍物联网发展的成本和诚信问题。政府数据信息在加密协议的基础上，结合区块链技术可以有效提升其工作效率、鲁棒性和安全性，确保数据共享交换平台上政府数据的安全。此外，政府应尽快采取行动，考虑数字化转型带来的机遇和威胁，选择最佳方式，减小数据信息风险，最大限度地提高采用新兴数字技术的价值。

## 4. 结论与展望

本文运用文献计量分析方法和 CiteSpace 可视化软件，对 2008~2022 年期间政府数据安全治理研究领域 WoS 收录的文献进行分析，揭示政府数据安全治理的研究现状、进展、热点和前沿。研究发现，自 2008 年以来，政府数据安全治理研究文献数量开始呈现出明显上升趋势，尤其是近三年发文数量更是快速增长，体现了国际学术界对于政府数据安全治理的重视和关注，再通过将公式计算所得的普莱斯曲线与文献年度累计发文量进行拟合，得出实际年度累计发文量与普莱斯曲线拟合较好，说明本文在检索策

略上比较合理，能够保证数据的查全率。在发文作者上，已形成了核心作者群，清华大学是该领域发文最多的机构，中国在政府数据安全治理研究领域的发文量处于世界首位，发文量排名前列的国家还有美国、印度、英格兰、韩国、澳大利亚等。

保障政府数据安全是一项复杂性的系统工程，本文基于前文的关键词词频、关键词聚类、关键词突现分析以及文献的阅读，应对政府数据安全面临的挑战，从两个方面对政府数据安全进行治理：“技术 + 政策”。

一是从科学技术角度。目前，物联网的安全性在人工智能领域引起极大关注，其被广泛应用于各种智能监控场景。然而由于模型的可解释性较弱，政府数据安全风险高，有学者基于区块链、数字水印、自学习和可解释性深度学习网络[27]等技术针对数据存储、数据传输、数据使用过程中面临的数据安全和风险问题，对数据来源进行身份鉴别和记录，防止未经授权或非法授权的数据访问和修改、恶意篡改数据或破坏数据，保障政府数据的安全性。阿伦•库马尔•亚达夫等介绍了一种 DPC2-CD 的安全架构和方法，它在公共云环境中提供安全的私有空间、执行云数据库的分布式处理和并发控制并使用介于客户端和云服务器之间的安全代理服务器，保证所提出方法中的数据机密性和完整性[28]。在数据加密方面，穆罕默迪，M 等利用 ElGamal 和密文策略属性加密(CP-ABE)算法[29]；赵柳荣等建立了 SIR 模型防止黑客入侵传播[30]；李倩文等考虑了多媒体数据传输中的版权保护问题，提出了一种基于压缩域多层嵌入的鲁棒可逆水印算法[31]；Gunjal 和 Mali 专注于通用水印系统的鲁棒性、不可察觉性、容量和安全问题，开发了一种非盲水印技术，以优化不可察觉性和鲁棒性，具有出色的嵌入能力和强大的安全特征[32]。各种技术方法的建立和应用可以有效保证数据生命周期各个阶段的安全运行，保障政府数据在授权范围内被安全访问。

二是政策制度角度。完善相关法律法规和建立监督管理机构，为政府的数据安全提供法律依据和政策保障。目前，不少国家和地区已经出台了相关政策和法规文件，但真正进入法律程序的还很少，大部分都是一些计划、意见和文件。不过仍有许多国家为政府数据安全的保障做了尝试和实践。在监督管理方面，为了应对缺乏任何解决数据安全问题的法律框架，美国在数据安全实践中成立了以联邦贸易委员会为主的监管机构[33]；此外，美国成为世界上首个建立首席信息官制度的国家，负责领导和监督整个联邦政府的 IT 支出[34]。在专业机构方面，英国政府专门设置了独立机构负责协调多方机构参与数据治理，同时还成立了专业咨询委员会和指导小组，形成独立审查机制，为政策标准的出台和落实提供专业支撑和建议反馈[35]；英国政府还通过建立第三方机构提供独立的大数据信托服务对政府数据进行治理；加拿大政府针对数字治理的需要，对其部门职能与机构设置进行了重置与调整，比如设置加拿大共享服务局，优化政府数据中心和网络系统[36]。这些都为我国政府数据安全治理提供新的思路和借鉴，将技术手段与政策手段有效结合保障政府数据安全，实现数据安全的全面有效治理。

## 参考文献

[1] 管晓宏, 沈超, 刘烃. 数据安全为何重要?应如何保障? [EB/OL]. 中国网信杂志. https://mp.weixin.qq.com/s/TZDboN8NBdAtSPu6XCJWTA, 2022-06-21.

[2] 马广惠, 安小米, 宋懿. 业务驱动的政府大数据平台数据治理[J]. 情报资料工作, 2018(1): 21-27.

[3] 张涛. 基于区块链的政府数据安全治理机制变革[J]. 河南工程学院学报(社会科学版), 2022, 37(3): 19-24.

[4] 黄璜. 美国联邦政府数据治理: 政策与结构[J]. 中国行政管理, 2017(8): 47-56.

[5] 谭必勇, 刘芮. 英国政府数据治理体系及其对我国的启示: 走向“善治” [J]. 信息资源管理学报, 2020, 10(5): 55-65.

[6] Prall, D. (2020) Better Local Government Data Security Can Prevent Property Fraud. The American City & County. https://www.americancityandcounty.com/2020/09/30/better-local-government-data-security-can-prevent-property-fraud/

[7] 陈悦. 引文空间分析原理与应用[M]. 北京: 科学出版社, 2014: 12.

[8] De Solla Price, D.J. (1961) Science since Babylon. Yale University Press, New Haven, 97.

[9] 苏屹, 郭家兴, 王文静. 基于科学计量学的国内区域创新研究热点和前沿分析[J]. 科学管理研究, 2019, 37(6): 77-83.

[10] 卢新元, 张恒, 王馨悦, 秦泽家. 基于科学计量学的国内企业知识转移研究热点和前沿分析[J]. 情报科学, 2019, 37(3): 169-176.

[11] 徐成, 赵宇翔, 朱庆华. 国外社会化媒体研究的文献计量分析[J]. 情报杂志, 2014, 33(3): 58-63.

[12] 佟瑞鹏, 梁明添, 李春旭. 《中国安全科学学报》载文特点及研究主题变化分析[J]. 中国安全科学学报, 2016. 26(1): 8-14.

[13] 田赛琦, 丁昇. 基于 WoS 和 CiteSpace 的制革研究知识图谱和进展分析[J]. 中国皮革, 2022, 51(6): 27-33+38.

[14] 马宁. 云环境下政府数据存取的法律困境及应对[J]. 暨南学报(哲学社会科学版), 2014, 36(1): 54-62.

[15] Minelli, M., Chambers, M. and Dhiraj, A. (2013) Big Data, Big Analytics: Emerging Business Intelligence and Analytic Trends for Today's Businesses. Elsevier, New York.

[16] Solove, D.J. (2013) Introduction: Privacy Self-Management and the Consent Dilemma. *Harvard Law Review*, **126**, 1880-1903.

[17] Mircea, M. (2012). Addressing Data Security in the Cloud. *World Academy of Science, Engineering and Technology*, **6**, 798-805.

[18] 戚学祥. 区块链技术在政府数据治理中的应用: 优势、挑战与对策[J]. 北京理工大学学报(社会科学版), 2018, 20(5): 105-111.

[19] 唐慧荣. 区块链技术运用助推精准扶贫[N]. 贵州日报, 2017-03-11(07).

[20] 蒋余浩, 贾开. 区块链技术路径下基于大数据的公共决策责任机制变革研究[J]. 电子政务, 2018(2): 26-35.

[21] Ashton, K. (2009) That "Internet of Things" Thing. *RFID Journal*. http://www.rfidjournal.com/articles/view?4986

[22] Goad, D., Collins, A.T. and Gal, U. (2021) Privacy and the Internet of Things—An Experiment in Discrete Choice. *Information & Management*, **58**, Article ID: 103292. https://doi.org/10.1016/j.im.2020.103292

[23] 龚惠群, 黄超. 物联网新兴产业的发展趋势分析[J]. 产业经济评论, 2023(2): 198-216.

[24] Piao, C.H., Hao, Y.P., Yan, J.Q. and Jiang, X.H. (2021) Privacy Preserving in Blockchain-Based Government Data Sharing: A Service-on-Chain (SOC) Approach. *Information Processing & Management*, **58**, Article ID: 102651. https://doi.org/10.1016/j.ipm.2021.102651

[25] Tan, E., Mahula, S. and Crompvoets, J. (2022) Blockchain Governance in the Public Sector: A Conceptual Framework for Public Management. *Government Information Quarterly*, **39**, Article ID: 101625. https://doi.org/10.1016/j.giq.2021.101625

[26] Luo, H. (2020) An Emergency Management System for Government Data Security Based on Artificial Intelligence. *Ingénierie des Systèmes d'Information*, **25**, 207-213. https://doi.org/10.18280/isi.250208

[27] Wu, B. and He, S. (2022) Self-Learning and Explainable Deep Learning Network toward the Security of Artificial Intelligence of Things. *The Journal of Supercomputing*, **79**, 4436-4467. https://doi.org/10.1007/s11227-022-04818-4

[28] Yadav, A.K., Raw, R.S. and Bharti, R.K. (2023) *DPC*$^2$*-CD*: A Secure Architecture and Methods for Distributed Processing and Concurrency Control in Cloud Databases. *Cluster Computing*, **26**, 2047-2068. https://doi.org/10.1007/s10586-022-03744-7

[29] Mohammadi, M., Rawassizadeh, R. and Sheikhtaheri, A. (2022) A Consumer-Centered Security Framework for Sharing Health Data in Social Networks. *Journal of Information Security and Applications*, **69**, Article ID: 103303. https://doi.org/10.1016/j.jisa.2022.103303

[30] Zhao, L.R., Zhou, X.Y. and Li, J. (2022) Information Security Decisions with Consideration of Hacker Intrusion Propagation. *Mathematical Problems in Engineering*, **2022**, Article ID: 3183121. https://doi.org/10.1155/2022/3183121

[31] Li, Q., Wang, X. and Pei, Q. (2022) Comparession Domain Reversible Watermarking Based on Multilayer Embedding. *Security and Communication Networks*, **2022**, Article ID: 4542705. https://doi.org/10.1155/2022/4542705

[32] Gunjal, B.L. and Mali, S.N. (2015) MEO Based Secured, Robust, High Capacity and Perceptual Quality Image Watermarking in DWT-SVD Domain. *SpringerPlus*, **4**, Article No. 126. https://doi.org/10.1186/s40064-015-0904-z

[33] Hurwitz, J. (2022) Data Security and the FTC's UnCommon Law. *Iowa Law Review*, **101**, 955-1021.

[34] 付羚. 数字化转型视域下的政府数据治理研究[J]. 中共南京市委党校学报, 2022(5): 74-81.

[35] 李重照, 黄璜. 英国政府数据治理的政策与治理结构[J]. 电子政务, 2019(1): 20-31.

[36] 谭溪. 加拿大数字政府治理改革实践及反思[J]. 中国行政管理, 2021(7): 140-146.