万方检测 原文标注报告【个人文献版-新文献】报告编号 PL-20210930-60DE99D5-BZ

送检文献信息

【题名】计算机导论报告 21009200038 江昱峰

作　　者：江昱峰

检测时间：2021-09-30 09:16:01

13.61%
总相似比

检测范围：

- [x] 中国学术期刊数据库
- [x] 优先出版论文数据库
- [x] 国内外重要学术会议论文数据库
- [x] 中国博士学位论文全文数据库
- [x] 中国优秀硕士学位论文全文数据库
- [x] 中国优秀报纸全文数据库
- [x] 互联网学术资源数据库
- [x] 学术网络文献数据库
- [x] 中国专利文献全文数据库
- [x] 特色英文文摘数据库
- [x] 中国标准全文数据库

详细检测结果

原文总字符数	检测字符数	参考文献相似比	辅助排除参考文献相似比	可能自引相似比	辅助排除可能自引相似比
6558	6149	5.53%	8.08%	0.00%	13.61%

相似文献列表（仅列举前10条）

序号	相似比(相似字符)	相似文献	类型	是否引用
1	5.53% 340字符	物联网网络层安全 于晓冉，李永思；《无线互联科技》；2013-05-25	期刊	是
2	2.08% 128字符	物联网研究与发展综述 胡向东；《数字通信》；2010-04-28	期刊	否
3	1.35% 83字符	物联网安全标准不可或缺 李侠；中国电子报；2012-04-27（版次：08版）	报纸	否
4	0.98% 60字符	人工智能发展应用过程的安全威胁分析及解决策略研究 裘玥, 北京市公安局石景山分局指挥处,北京100043; 李思其, 云南警官学院,云南昆明650223；《第33次全国计算机安全学术交流会》；2018-10-10	会议	否
5	0.49% 30字符	移动雾计算中基于强化学习的通信安全关键技术研究 孟远（导师：涂山山）；北京工业大学，硕士（专业：计算机科学与技术）；2020	学位	否
6	0.47% 29字符	基于安卓的ATM机物联网软件平台的设计与实现 吴昊（导师：董立岩）；吉林大学，硕士（专业：计算机应用）；2020	学位	否
7	0.33% 20字符	基于SOA的物联网智慧服务系统的设计与实现 陈杨（导师：江凌云）；南京邮电大学，硕士（专业：电子与通信工程）；2016	学位	否
8	0.31% 19字符	上海工业互联网，以技术助力复工复产 ；文汇报；2020-04-04（版次：02版）	报纸	否
9	0.28% 17字符	2016物联网安全白皮书 信息安全与通信保密杂志社梆梆安全研究院；《信息安全与通信保密》；2017-01-01	期刊	否
10	0.26% 16字符	被遗忘权研究 刘雨蒙（导师：方勇男;金光锡）；延边大学，硕士（专业：法律硕士（非法学））；2020	学位	否

原文标注

计算机导论报告————物联网安全技术21009200038 江昱峰

目录

摘要、Abstract……3

0引言……4

1物联网概述……4

2物联网技术现有的安全问题及相应需求……5

2.1物联网技术的安全问题……5

2.1.1物联网环境下信息安全威胁……5
2.1.2物联网环境下公民个人信息管理不完善……6
2.2物联网技术的现存需求……6
3物联网安全技术的现状……7
4物联网安全技术未来发展方向及个人理解思考……9
4.1物联网安全技术未来发展方向……9
4.2对于物联网安全技术未来发展的个人理解思考……9
5结语……9

[摘要]:

本文从物联网安全技术问题现存的问题、需求出发，在介绍了物联网概念的基础上，以物联网三大层面的角度为主、个人角度为辅深入挖掘了物联网安全技术各方面存在的问题、需求，同时分析了物联网安全技术的现状、优缺点及未来发展方向，并提出了个人的思考。

关键词：物联网安全；问题需求；技术现状；发展趋势

[Abstract]:

Starting from the existing problems and needs of the security technology of the Internet of things, this paper introduces the concept of the Internet of things, mainly from the perspective of the three levels of the Internet of things, supplemented by the personal perspective, deeply excavates the problems and needs of the security technology of the Internet of things, and analyzes the current situation, advantages and disadvantages and future development direction of the security technology of the Internet of things, And put forward personal thinking.

Keywords:Internet of things security; Problem demand; Technical status; Development trend

0引言

随着5G、大数据、物联网、云计算、人工智能、新技术的发展，全球进入万物互联的智能时代，同时驱动了海量数据的爆炸式增长。在许多技术中，5G是通信基础设施；大数据是一个应用程序；人工智能以及云计算用于提高效率；物联网是一个平台，而这些技术只能在结合互联网时发挥最大的作用。物联网给我们带来了前所未有的发展速度，也融入了生活的方方面面。智能家居、智能交通、智能医疗、智能城市是物联网在各领域的互联网，物联网是人类社会的真正领导。然而，随着物联网的蓬勃发展，安全问题的形势也很严峻。未来很长一段时间，物联网安全威胁都将是最大的安全威胁之一，物联网安全支出在信息安全整体市场的占比也将快速提升。由于物联网全面感知的特点，大量的个人信息被收集、传输，以及在物联网中处理，因此通过物联网所带来的个人信息安全问题是比较复杂的、多元化的，且不易获得有效的监管。本文就将从物联网安全的问题、需求谈起，全面地探讨物联网。

物联网概述物联网是指各种信息传感器，RFIT，全球定位系统，红外传感器，激光扫描仪和其他设备和技术，并收集需要监控，连接，交互和收集其声音的任何对象或过程。 通过各种可能的网络访问，通过各种可能的网络访问，实现各种可能的网络，实现对象的智能连接，识别和管理的各种需求的信息。 物联网是一种基于互联网的信息载体，传统电信网络，其允许独立地形成的所有常见物理对象以互通互操作性。

物联网技术现有的安全问题及相应需求

2.1物联网技术的安全问题

2.1.1物联网环境下信息安全威胁

（1）感知层信息安全威胁

物联网感知层是信息采集的关键部分，用于全面感知和收集外界信息，是物联网系统中数据的来源。由于感知层有着不可计数的感知终端，在很多情况下，感知层设备和传感器是在露天公共场所，处于无人值守的环境，或者设备获取数据时没有安全防护措施，攻击者可能会对传感器等进行物理破坏，导致终端没办法正常工作，也有可能攻击者会盗取这些终端设备，并对这些设备进行破解，设备中的个人敏感信息就容易被非法获取进而利用数据进行其他违法犯罪活动。当前，大量的感知设备直接暴露于互联网，这些感知设备无法支持复杂的安全功能，可能会存在安全漏洞，攻击者可以利用各种方式攻击设备，对设备进行远程控制，监听用户信息，窥探用户的隐私。

现在被广泛使用的个人电子设备终端由于嵌入了 RFID 标签、二维码而具有感知功能，攻击者在用户没有察觉的情况下对设备进行扫描、 追踪、定位，分析统计用户的行为习惯，个人信息被严重泄漏。 根据 PaloAltoNetworks（派拓网络）的威胁情报团队 Unit42 发布的《2020 年物联网威胁报告》，98%的物联网设备流量未加密，个人信息和机密数据被暴露在网络上。57%的物联网设备容易受到中、重度攻击，成为攻击者最先下手的目标。这份报告是对美国物联网设备的网络安全进行的统计和总结，值得正在高速发展的中国物联网行业借鉴。 近年来警方侦破了多起破解家庭摄像头软件的犯罪案件，不法分子在网上售卖破解软件，通过这些软件能够远程控制家庭摄像头， 非法购买者可以利用摄像头进行偷窥，严重侵犯了公民的个人隐私。很多家用甚至公共场合的摄像头也存在使用弱口令就可以打开的问题，这类摄像头很容易入侵，存在严重的安全隐患。

（2）网络层信息安全威胁

物联网网络层安全威胁主要来自以下几个方面：

①终端本身是安全的。随着物联网终端的智能越来越多，事情互联网更加丰富，也增加了终端传染性病毒，特洛伊木马或恶意侵入的渠道。与此同时，网络终端自己的系统平台缺乏！整体保护和验证机制，平台硬件和软件模块易于被攻击者篡改，一旦窃取或篡改，存储私人信息将面临泄漏的风险；

②承载网络信息传输安全性。内容网的轴承网络是多网络叠加开放网络。随着网络融合的加速和网络结构的增加，雷霆互联网面临基于无线和有线链路的更多威胁。攻击者可以窃取，篡改或删除链接上的数据，并伪装到网络实体，以拦截业务数据并分析网络流量；

③核心网络安全未来。所有基于IP的移动通信网络和互联网以及下一代互联网将是物联网网络的核心向量。对于完整的IP开放网络，它将面临传统的DOS攻击，DDOS攻击，假冒攻击和其他网络安全威胁，以及物联网的业务节点数量将大大超过以前的服务网络，这将携带大型服务网络数据传输量。网络堵塞，生成拒绝服务攻击。

（3）应用层信息安全威胁

物联网应用层负责对网络层传送过来的数据进行存储、分析、管理和应用，随着物联网与各行业的深度融合，出现形式各异的业务平台，产生广泛的智能化应用。由于业务系统的各种数据存储在应用层，用户数据高度集中，容易成为攻击者的攻击目标。应用层的各类业务系统与用户联系最紧密，会包含大量的公民个人信息，业务平台通过数据挖掘、智能分析等手段对数据进行处理后，挖掘出未经用户许可的敏感信息，释放出用户的商业价值，如生活习惯、出行路线、消费偏好、健康状况、社会关系等信息，如果信息被攻击者窃取，可能会被利用进行精准诈骗、行为跟踪等等，将严重威胁公民的人身安全和财产安全

2.2.2物联网环境下公民个人信息管理不完善

随着物联网应用深入到众多行业领域，在各个行业中都存在大量的个人信息，过度收集个人信息的情况普遍存在，收集的信息可能会涉及用户的个人隐私，也没有告知用户信息被收集后用在何处，信息是否有使用期限，甚至有些应用故意留下漏洞，在用户没有明确许可的情况下，获取用户的个人信息。作为收集数据的物联网企业，如果不妥善保存和管理用户信息，对信息的防范保护缺乏相关的技术手段，可导致个人信息被轻易泄露。还有些行业监管体系不完善，行业不自律，会出现内部的从业人员泄露用户的个人信息。相对于攻击者的恶意攻击，内部人员信息泄露更加隐秘，难以发现。目前针对物联网个人信息安全保护的专项法律法规缺失，虽然我国近年来有多部涉及信息保护的法律法规，但是这些法律条文分散在各个法律规定以及各项部门规章里，缺乏针对个人信息保护的专门的立法，缺少行业在信息的收集、使用和存储的指导性规范，当公民个人信息安全受到侵犯时，依然无法可依。亟待出台《个人信息安全保护法》，制定公民个人信息的保护规范。 我国民众的安全意识也需要进一步提高，很多人对于物联网的安全问题缺乏直观认识，不知道自己所连接的物联网设备会泄露自己的隐私信息。有些用户对智能家居设备不设置密码保护，或者采用设备出厂时的默认密码，导致入侵者可以轻易控制设备，个人隐私数据被泄露，将严重威胁个人的信息安全。

2.2物联网技术的现存需求

物联网对安全的需求可以涵盖以下几个方面：

（1）在运营商网络中转移安全性。需要确保在运营商网络传输期间未泄漏数据内容，篡改和数据流不是非法获取的；

（2）携带网络安全保护。互联网需要解决易受攻击的传输点或核心网络设备的非法攻击，以便安全；

（3）终端和异构网络认证认证。提供轻量级认证认证和访问控制到事物终端终端，实现异构网络连接，身份验证管理等的身份认证，认证管理，认证管理等；

（4）异构网络下的终端安全访问。物联网应用程序行业带有各种承载网络，如互联网，移动通信网络，WLAN网络，需要改进网络访问技术和网络架构，以满足事务互联网的安全应用需求；

（5）物联网应用网络是统一协议堆栈需求。事情互联网需要统一的协议栈和相应的技术标准，通过篡改协议，协议漏洞来消除安全风险威胁网络应用：

（6）大型终端分布式安全控制。物联网的大规模部署应用终端对网络安全控制系统，安全控制和应用服务，统一部署，安全测试，紧急联动，安全审核等进行了新的安全要求。

物联网安全技术的现状物联网安全行业在我国起步较晚，受制于物联网安全技术的不成熟以及物联网应用的普及度不高，使得中国物联网安全行业发展缓慢，2015年我国物联网安全行业市场规模仅39.2亿元。伴随着物联网安全技术的突破，我国物联网安全行业发展迅速。再加上由于物联网普及带来的安全问题，使得对于物联网安全的需求迅速增长。根据数据显示，2019年我国物联网安全行业市场规模为128.8亿元，2015-2019年年均复合增长率达到34.6%。

（数据来源：IDC，华经产业研究院整理）（相关报告：华经产业研究院发布的《2020-2025年中国物联网安全行业发展潜力分析及投资方向研究报告》）在我国物联网安全行业用户中，政府是最重要的参与者，用户占比达到30%；其次为金融领域和电力领域，占比分别达到15%和11%；而能源、交通、安防领域都是基础领域，用户占比相差不大，分别为9%、8%和8%；而制造和物流用户占比分别为5%和2%。

（数据来源：东方财富，华经产业研究院整理）在“万物互联”时代，智能摄像头是实现智能监控的基本硬件，智能摄像头凭借其直观可视性和价格低廉等优势成为应用广泛的智能硬件。据360攻防实验室发布的《中国智能家庭摄像头安全状况评估报告》显示，目前中国近80%的家庭智能摄像头因设备安全缺陷如数据传输未加密、APP未安全加固、代码逻辑存在缺陷、硬件存在调试接口、可横向控制等原因导致用户信息泄露，其中摄像头暴露事件较集中的省份为辽宁、广东和吉林，暴露数量分别为27.5万台、16.8万台和11.5万台。智能摄像头的暴露将会带来严重的安全问题，影响居民的生命财产安全，因此解决智能摄像头暴露问题是现在物联网安全行业的主要需求，也是拉动物联网安全行业增长的主要动力。

（数据来源：360，华经产业研究院整理）物联网安全技术未来发展方向及个人理解思考

4.1物联网安全技术未来发展方向

（1）物联网安全由“被动”走向“主动”

物联网安全事件频发，针对物联网业务系统的攻击形式呈现多样化，传统的防御手段难以满足日益增长的安全防护需求。伴随物联网攻防技术的发展，物联网安全防护手段将由“被动防御” 向“主动防护” 转移，对物联网应用系统可能存在的安全漏洞以及新型攻击手段给予主动防护，在物联网供给链条中寻找最佳防御点，采取针对性的防御技术，构建有效的物联网安全防护体系将成为行业重要的发展趋势。

（2）建立健全物联网安全标准体系

物联网安全的合规性驱动行业发展，但目前中国物联网安全市场尚处于早期发展阶段，各领域安全标准尚未统一，物联网安全产品落地存在困难。伴随网络安全等级保护的正式发布，政府对物联网安全作出详细分级安全要求，覆盖安全物理环境、安全区域边界、安全计算环境、抗数据重放、数据融合处理、安全运维管理6个方向。现阶段，不同的企业和机构已初步建立各自的技术方案，但核心技术研发方面缺乏协同，方案间缺乏统一的规划和接口，企业业务以定制项目为主，缺乏可复制性，企

业之间没有标准接口，无法共享资源。

物联网安全标准的建立有望加速行业合规发展及物联网安全产品在各领域的商业化落地，因此建立健全物联网安全标准体系将成为物联网安全行的重要发展方向。

华经情报网隶属于华经产业研究院，专注大中华区产业经济情报及研究，目前主要提供的产品和服务包括传统及新兴行业研究、商业计划书、可行性研究、市场调研、专题报告、定制报告等。涵盖文化体育、物流旅游、健康养老、生物医药、能源化工、装备制造、汽车电子等领域，还深入研究智慧城市、智慧生活、智慧制造、新能源、新材料、新消费、新金融、人工智能、“互联网+”等新兴领域。

4.2对于物联网安全技术未来发展的个人理解思考

任何技术的出发点都是为了人类生活的便利快捷以及自然、社会与世界的和谐发展。而它们在发展的过程中总会遇到一些问题。但总的来说，应用需求总是推动技术进步的不竭动力，建立人与物理环境间便捷联系的需求就是未来物联网发展不竭动力的源泉，环境的“智能化”体现了科技为人类服务的本质，也是物联网的基本内涵，在广大科技工作者以及政府和相关应用部门的不懈努力下，美妙的“物联网时代”正在快步向我们走来！

结语

在万物互联的时代，物联网安全形势严峻，物联网的个人信息安全已成为物联网高速发展需要解决的重要课题。本文基于物联网的三个逻辑层次分析了物联网面临的信息安全威胁，以及个人信息泄露的风险，从物联网技术层面与物联网安全管理层面，以及区块链技术应用到物联网等方面进行探讨，提出针对当前物联网信息安全问题的保护措施，促进物联网的信息安全，加强公民个人信息的保护。

参考文献

[1]百度百科-物联网.

[2]曹美荣,张辉.物联网环境下公民个人信息安全研究[J].网络安全技术与应用,2021(09):19-21.

[3]于晓冉,李永思.物联网网络层安全[J].无线互联科技,2013(05):22.

[4]华经情报网（主要责任者） 物联网安全行业发展现状及趋势分析，物联网安全由被动走向主动.搜狐网.