DOI:10.3969/j.issn.1009-6868.2016.01.004
网络出版地址:http://www.cnki.net/kcms/detail/34.1228.TN.20151117.1514.012.html

云时代下的大数据安全技术

Security Technology of Big Data in the Cloud Era

杨曦/YANG Xi [1,2]
GUL Jabeen [1]
罗平/LUO Ping [1]

(1. 清华大学 信息系统安全教育部重点实验室,北京 100084;
2. 福州大学 阳光学院计算机工程系,福州 350015)
(1.The Key Laboratory for Information System Security, Ministry of Education, Tsinghua University, Beijing, 100084, China;
2. Computer Engineering Department, Sushine College of Fuzhou University, Fuzhou 350015, China)

中图分类号:TN929.5 文献标志码:A 文章编号:1009-6868 (2016) 01-0014-005

摘要: 认为云计算结合大数据,是时代发展的必然趋势。提出了保障大数据安全的方法和技术,方法包括:构建云环境下的大数据信息安全体系,建立并研究基于Hadoop的大数据安全架构等;技术包括:基于大数据的威胁发现技术、大数据真实性分析技术、基于大数据的认证技术、基于大数据的安全规则挖掘技术,以及防范高级持续性威胁(APT)攻击的技术。认为大数据带来许多新的安全问题和挑战,但它本身也是解决问题的重要手段,需要进一步地研究。

关键词: 大数据;云计算;大数据安全;APT攻击;数据挖掘

Abstract: The combination of cloud computing and big data is an inevitable trend. In this paper, methods and techniques for ensuring the security of large data are presented. These methods include: building a large data information security system in a cloud environment and establishing and studying the big data security architecture based on Hadoop. These techniques include: threat discovery based on big data, big data authenticity analysis, authentication based on big data, security rule mining based on big data, and preventing advanced persistent threat (APT) attack. Big data creates many new security problems and challenges, but it is also an important means to solving the problem, which needs for further research.

Key words: big data; cloud computing; big data security; APT attack; data mining technology

随着云时代的来临,大数据也吸引了越来越多学术界和工业界的关注。从20世纪90年代“数据仓库之父”Bill Inmon率先提出“大数据”的概念,到2011年麦肯锡全球研究院(MGI)发布了关于大数据的详尽报告,直至2012年美国奥巴马政府公布了“大数据研发计划”,才使得大数据真正成为许多学科的重点研究课题。大数据科学的基础研究已经成为当今社会的研究热点。英国牛津大学教授维克托·迈尔·舍恩伯格,在他的《大数据时代:生活、工作与思维的大变革》一书中,深刻地阐述了大数据所带来的三大变革,即思维变革、商业变革和管理变革。大数据带来更多的是思维变革——样本数据或局部数据向全体数据的变革,结果数据向过程数据的变革,静态存储数据向动态流处理数据的变革。

收稿日期:2015-11-10
网络出版时间:2015-11-17
基金项目:国家自然科学基金(60973142);福建省教育厅A类科技项目(JA14358)

随着大数据技术的不断发展,许多传统的信息安全技术也受到了挑战。在大量数据产生、收集、存储和分析的过程中,既会涉及一些传统安全问题,也会涉及一些新的安全问题,并且这两类问题会随着数据规模、处理过程、安全要求等因素而被不断放大。而大数据的4V(大量、高速、多样、真实性)+1C(复杂)特征,也使得大数据在安全技术、管理等方面面临新的安全威胁与挑战[1]。

1 大数据安全技术发展现状

谈到大数据,不可避免地就要提及云计算技术,它们就像一枚硬币的正反面一样密不可分。云计算结合大数据,是时代发展的必然趋势。云计算为大数据提供了存储场所、访问渠道、虚拟化的数据处理空间,具有盘活数据资产价值的能力。另一方面,大数据技术通过挖掘价值信息[2]进行预测分析、策略决断,为国家、企业甚至个人提供决策和服务。

作为一个云化的大数据架构平台,Hadoop自身也存在着云计算面临的安全风险,企业需要实施基于身份验证的安全访问机制,而Hadoop派生的新数据集也同样面临着数据加密问题。云端大数据从使用频率上有静态数据加密机制和动态数据加密机制两种[3]。静态数据加密机制与传统加密一样,有对称加密算法和非对

称加密算法两种。而动态数据加密机制方面近年来则有较多的论述，较为常用的是同态加密机制[4]。对加法同态的加密算法有 Paillier 算法[5]，对乘法同态的加密算法有 RSA 算法，还有对加法和简单标量乘法同态的加密算法，如 IHC 和 MRS 算法[6]。Craig Gentry 提出一种基于理想格的全同态加密算法[7]，实现了全同态加密所有属性的解决方案。

同样，大数据依托的非关系型数据库（NoSQL）技术没有经过长期发展和完善，在维护数据安全方面也未设置严格的访问控制和隐私管理，缺乏保密性和完整性特质。另一方面，NoSQL 对来自不同系统、不同应用程序及不同活动的数据进行关联，也加大了隐私泄露的风险。大数据时代，想屏蔽外部数据商挖掘个人信息是不可能的，大数据隐私问题堪忧。Itani 提出的协议能够在云计算环境下保证用户的隐私[8]，Creese 的方案有效地解决了企业云部署中的隐私安全问题[9]。除了常见的基于加密体制的数据存储和数据处理的隐私性保护方案外，A. Parakh 等于 2011 年和 2013 年分别提出了基于空间有效性的机密共享隐式机制[10]及运用隐式机制的云端计算机制[11]。针对非结构化数据（比如社交网络产生的大量数据）的隐私保护技术也是云时代下大数据安全隐私保护的重大挑战，典型的匿名保护需求为用户标识匿名、属性匿名（也称点匿名）及边匿名（用户间关系匿名）。目前边匿名方案大多是基于边的增删[12]，还有一个重要思路是基于超级节点对图结构进行分割和聚集操作[13]。

2 基于大数据的安全技术及发展趋势

新形势下的大数据安全也面临诸多新的挑战，在大数据产业链的各个环节，安全问题无处不在。面对一系列的安全风险和关键问题，如何保障大数据安全，并在信息安全领域有效利用，是学术界和工业界都需要认真对待和解决的问题。

2.1 构建云环境下的大数据信息安全体系

只有在正确完整的安全体系指导下，大数据信息安全建设所需的技术、产品、人员和操作等才能真正发挥各自的效力。大数据应用过程通常划分为采集、存储、挖掘、发布 4 个环节，它们的安全性可通过下面一些技术和方法实现：

（1）数据采集阶段的安全问题主要是数据汇聚过程中的传输安全问题，需要使用身份认证、数据加密、完整性保护等安全机制来保证采集过程的安全性。传输安全主要用到虚拟专用网络（VPN）和基于安全套接层协议 VPN（SSL VPN）技术。

（2）数据存储阶段需要保证数据的机密性和可用性，提供隐私保护、备份与恢复技术等。这个阶段可能用到的技术有：基于数据变换的隐私保护技术（包括随机化、数据交换、添加噪声等）、基于数据加密的隐私保护技术、基于匿名化的隐私保护技术（通常采用抑制、泛化两种基本操作）、静态数据加密机制（数据加密标准（DES）、高级加密标准（AES）、IDEA、RSA、ElGamal 等）、动态数据加密机制（同态加密）、异地备份、磁盘阵列（RAID）、数据镜像、Hadoop 分布式文件系统（HDFS）等。

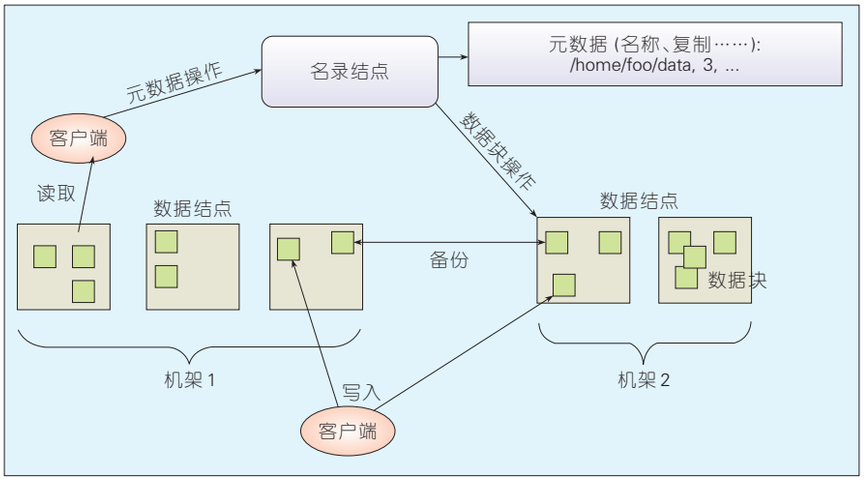
（3）数据挖掘阶段需要认证挖掘者的身份、严格控制挖掘的操作权限，防止机密信息的泄露。这个阶段涉及到的技术有：基于秘密信息的身份认证、基于信物的身份认证技术、基于生物特征的身份认证技术、自主访问控制、强制访问控制、基于角色的访问控制等。

（4）数据发布阶段需要进行安全审计，并保证可以对可能的机密泄露进行数据溯源。这个阶段的技术可能涉及到：基于日志的审计技术、基于网络监听的审计技术、基于网关的审计技术、基于代理的审计技术、数据水印技术等。

2.2 基于 Hadoop 的大数据安全架构

Hadoop 是一种分布式数据和计算的框架，在全球范围内已成为大数据应用最为广泛的技术架构。当前，Hadoop 已成为工业界和学术界进行云计算应用和研究的标准平台。分布式文件系统使大规模并行计算成为可能，但堆栈各层的集成以及数据节点与客户端/资源管理机构之间通信，都会引入新的安全问题。图 1 是 Hadoop 核心 HDFS 的架构，在不破坏大数据集群的基本功能及大数据本身必要特点的前提下，我们先来分析这种架构下的安全问题及隐患并给出相应安全解决建议。

在高度分布式数据集群中，很难验证异构平台之间安全的一致性，即不同的数据结点的数据安全的整体性和一致性是分布式计算的痛点。而与传统集中式数据安全模型不同的是，大数据集群内的数据是流动的，有多个副本，在不同节点间移动以确保冗余和弹性的机制导致数据很难及时、准确地定位存储位置，无法获知数据备份个数，这加大了副本安全保护机制设计上的难度。对于数据访问，大多数大数据环境提供了 schema 级别的访问控制，但没有更细的粒度，虽然在大数据环境中可以借鉴安全标签和其他高级属性，但需要应用设计者将这些功能集成到应用和数据存储中去。对于节点间的通信，Hadoop 和绝大多数组件之间的通信是不安全的，它们使用传输控制协议（TCP）/IP 之上的远程过程调用协议（RPC），并没有嵌入安全传输层协议（TSL）和 SSL 等安全机制。另外，客户端可以直接与资源管理者及节点进行交互，增加了恶意代码或链接发送的概率，也难以保证客户端免受数据节点的攻击。最后，最为重要的是大数据栈自身设计并没有考虑安全机制。这些都是基于 HDFS 架构的



▲图 1 Hadoop 的 HDFS 架构

大数据环境的安全隐忧。

基于 Hadoop 的大数据架构，其安全机制可以通过下面一些方法和技术得以保证：

（1）使用 Kerberos 进行节点验证。Kerberos 是一个最有效的安全控制措施之一，并且可以集成到 Hadoop 基础设施中。其可有效验证服务间通信，阻断集群中的恶意节点和应用程序，保护 Web 控制台的访问，使得管理通道难以被攻击。

（2）对于恶意客户端发起的获取文件请求，可以通过使用文件层加密对数据加以保护。被恶意访问的文件是不可读的磁盘映像，且文件层加密提供一致安全保护，有些产品甚至提供内存加密保护。

（3）使用密钥管理服务分发密钥和证书，并为每个组应用程序和用户设置不同密钥，可以提高密钥的安全性，防止文件加密的失效。

（4）在节点之间、节点与应用程序之间使用 SSL/TLS 组件实现安全通信，设计、集成有效的安全通信机制和现成组件。

2.3 基于大数据的威胁发现技术

由于大数据分析技术的出现，企业可以超越以往的“保护—检测—响应—恢复”（PDDR）模式，更主动地发现潜在的安全威胁。“棱镜”计划也可以被理解为应用大数据方法进行安全分析的成功故事。通过收集各个国家各种类型的数据，利用安全威胁数据和安全分析形成系统方法发现潜在危险局势，在攻击发生之前识别威胁。基于大数据的威胁发现技术可以使分析内容的范围更大，通过在威胁检测方面引入大数据分析技术，可以更全面地发现针对企业数据资产、软件资产、实物资产、人员资产、服务资产和其他为业务提供支持的无形资产等各种信息资产的攻击。另一方面，基于大数据的威胁发现技术可以使分析内容的时间跨度更长，现有的威胁分析技术通常受限于内存大小，无法应对持续性和潜伏性攻击。而引入大数据分析技术后，威胁分析窗口可以横跨若干年的数据，因此威胁发现能力更强，可以有效应对高级持续性威胁（APT）类攻击。基于大数据的威胁分析，我们可以对攻击威胁进行超前预判，能够寻找潜在的安全威胁，对未发生的攻击行为进行预防。而传统的安全防护技术或工具大多是在攻击发生后对攻击行为进行分析和归类，并做出响应。传统的威胁分析通常是由经验丰富的专业人员根据企业需求和实际情况展开，然而这种威胁分析的结果很大程度上依赖于个人经验。同时，分析所发现的威胁也是已知的。大数据分析的特点是侧重于普通的关联分析，而不侧重因果分析，因此通过采用恰当的分析模型可发现未知威胁。

2.4 大数据真实性分析技术

目前，基于大数据的数据真实性分析被广泛认为是最为有效的方法。基于大数据的数据真实性分析技术能够提高垃圾信息的鉴别能力。一方面，引入大数据分析可以获得更高的识别准确率。例如，对于点评网站的虚假评论，可以通过收集评论者的大量位置信息、评论内容、评论时间等进行分析，鉴别其评论的可靠性。如果某评论者为某品牌多个同类产品都发表了恶意评论，则其评论的真实性就值得怀疑。另一方面，在进行大数据分析时，通过机器学习技术可以发现更多具有新特征的垃圾信息。然而该技术仍然面临一些困难，主要是虚假信息的定义、分析模型的构建等。

云时代的未来必将涌现出更多、更丰富的安全应用和安全服务。对于绝大多数信息安全企业来说，更为现实的方式是通过某种方式获得大数据服务，结合自己的技术特色领域，对外提供安全服务。一种未来的发展前景是：以底层大数据服务为基础，各个企业之间组成相互依赖、相互支撑的信息安全服务体系，总体上可以形成信息安全产业界的良好生态环境。

2.5 基于大数据的认证技术

传统的认证技术主要通过用户所知的秘密（例如口令），或者持有的凭证（例如数字证书）来鉴别。这样就会存在问题：首先，攻击者总是能够找到方法来骗取用户所知的秘密或窃取用户持有的凭证，从而轻松通过认证；其次，传统认证技术中认证方式越安全往往意味着用户负担越重（例如携带硬件 USBKey），如果采用先进的生物认证技术，又需要设备具有生物特征识别功能，从而限制了

这些先进技术的使用。如果在认证技术中引入大数据分析则能够有效地解决这两个问题。基于大数据的认证技术指的是收集用户行为和设备行为数据，并对这些数据进行分析，获得用户行为和设备行为的特征，进而通过鉴别操作者行为及其设备行为来确定其身份。这与传统认证技术利用用户所知秘密、所持有凭证或具有的生物特征来确认其身份有很大不同。这样，攻击者很难模拟用户行为特征来通过认证，因此更加安全，同时又减小了用户认证负担，可以更好地支持各系统认证机制的统一。

2.6 基于大数据的安全规则挖掘技术

在Internet网络中，为保证网络安全，会引入防火墙技术和入侵检测技术等。在这些技术中，通常是通过建立一套安全规则或过滤规则达到其安全目标，而这些规则的建立传统方法是通过专家知识系统。在大数据时代，这些安全规则可以通过数据挖掘技术或方法实现。

聚类分析是数据挖掘中的一项重要技术，根据在数据中发现的描述对象及其关系的信息，将数据对象分组。组内相似性越大，组间差别越大，聚类效果就越好。

K-means算法作为聚类分析中的一种基本方法，由J.MacQueen于1967年首次提出[14]，由于其容易实现，时间复杂度与数据规模接近线性，并且能够快速地收敛到局部最优值，因此成为最广泛应用的聚类算法[15]。然而K-means算法也存在较为明显的缺陷，其中有以下两点：

（1）K-means算法需要人为确定聚类数K和选取初始质心集，其聚类结果的好坏明显受到初始化条件的影响[16-18]，即选取不同的K值和初始质心集会得到不同的聚类结果。

（2）K-means算法仅适用于数据项全是数字的情况。对非数字数据进行聚类分析是一个特别棘手的问题[19]，这在很大程度上限制了K-means算法的应用范围。

针对问题（1），Ester M等提出了基于密度的聚类方法DBSCAN[20]，该算法以及以此为基础的一些改进算法[17-18]采用基于密度的自动聚类，避免了对初始条件的随机选取，在一定程度上解决了K-means算法对初始条件敏感的问题。然而，由于基于密度的聚类算法时间复杂度通常较高，在处理大规模数据集时会出现瓶颈；同时在对于非数字数据集的聚类过程中，采用传统的基于密度的聚类算法往往会造成聚类失效问题。

针对以上问题，在借鉴K-means算法框架的基础上，文献[21]提出一种基于“预抽样-次质心”的密度聚类算法，采用预抽样的方法将算法时间复杂度控制为线性，同时通过引入次质心的概念，解决聚类失效问题。分析表明该算法能很好地克服K-means算法的初始条件敏感性和一般密度聚类算法的聚类失效问题，实现较为理想的聚类结果。

2.7 防范APT攻击的技术

APT攻击是大数据时代面临的最复杂的信息安全问题之一，而大数据分析技术又为对抗APT攻击提供了新的解决手段。APT具有极强的隐蔽性，且潜伏期长、持续性和目标性强，技术高级，威胁性也大。APT攻击检测方案通常有沙箱方案、异常检测、全流量审计、基于深层协议解析的异常识别、攻击溯源等。在APT攻击检测中，存在的问题包括：攻击过程包含路径和时序；攻击过程的大部分貌似正常操作；不是所有的异常操作都能立即检测；不能保证被检测到的异常在APT过程的开始或早期。基于早期记忆的检测可以有效缓解上述问题，既然APT是在很长时间发生的，我们的对抗也要在一个时间窗内来进行，并对长时间、全流量数据进行深度分析。APT攻击防范策略包括防范社会工程、通过全面采集行为记录避免内部监控盲点、IT系统异常行为检测等。

3 结束语

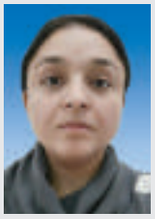
大数据带来许多新的安全问题和挑战，但大数据本身也是解决问题的重要手段，它就像一把双刃剑，既需要研究合适的“盾”来保护大数据，也需要研究如何用好大数据这根“矛”。战略资询公司麦肯锡认为：大数据将会是带动未来生产力发展、科技创新及消费需求增长的指向标，它以前所未有的速度，颠覆人们探索世界的方法，驱动产业间的融合与分立。大数据已成为各个国家和领域关注的重要战略资源，可能对国家治理模式、企业决策、组织业务流程、个人生活方式都将产生一系列长远、巨大的影响。

参考文献
[1] MANADHATA P K. Big Data for Security: Challenges, Opportunities, and Examples [C]// Proceedings of the 2012 ACM Workshop on Building Analysis Datasets and Gathering Experience Returns for Security, Raleigh, North Carolina, USA, 2012
[2] YU S C, WANG C, REN K, et al. Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing [C]// Proceedings of the INFOCOM'10,the 29th conference on Information communication, Piscataway, USA, 2010: 534-542
[3] BELARE M and ROGAWAY P. Introduction to Modern Cryptography [J]. Ucsd Cse, 2005: 207
[4] GENTRY C, HALEVI S, SMART N P. Homomorphic Evaluation of The AES Circuit [M]. Germany: Springer Berlin Heidelberg, 2012
[5] CATALANO D. Paillier's Cryptosystem Revisited [C]// in Proceedings of the 8th ACM conference on Computer and Communications Security, PA, USA, 2001: 206-214
[6] BENDLIN R, DAMGARD I, ORLANDI C, et al. Semi-Homomorphic Encryption and Multiparty Computation [M]. Germany: Springer Berlin Heidelberg, 2011
[7] GENTRY C. A Fully Homomorphic Encryption Scheme [D]. Standford University, 2009
[8] ITANI W, KAYSSI A, CHEHAB A. Privacy As a Service: Privacy-Aware Data Storage and

Processing in Cloud Computing Architectures [C]// Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing, Washington DC, USA, 2009:711–716.doi: 10.1109/DASC.2009.139
[9] CREESE S, HOPKINS P, PEARSON S, et al. Data Protection–Aware Design for Cloud Services [M]. Germany: Springer Berlin Heidelberg, 2009
[10] PARAKH A, KAK S. Space Efficient Secret Sharing for Implicit Data Security [J]. Information Science, 2011, 181(2): 335–341
[11] PARAKH A, MAHONEY W. Privacy Preserving Computations Using Implicit Security [C] // Proceedings of the 22nd International Conference on Computer Communications and Networks (ICCCN), Nassau, Bahamas, 2013: 1–6. doi: 10.1109/ICCCN.2013.6614172
[12] ZHANG L J, ZHANG W N. Edge Anonymity in Social Network Graphs [C] // Proceedings of the International Conference on Computational Science and Engineering (CSE'09),Vancouver, Canada, 2009:1–8
[13] MICHAEL H A, GEROME M, DAVID J, et al. Resisting Structural Re–identification in Anonymized Social Networks[C] // Proceedings of the 34th International Conference on Very Large Data Bases (VLDB'2008), Aucklnad, New Zealand, 2008: 102–114
[14] MACQUEEN J. Some Methods for Classification and Analysis of Multivariate Observations. [C] // Proceedings of the Fifth Berkeley Symposium on Mathematical Statistics and Probability, Oakland, USA, 1967: 281–297
[15] JAIN A K. Data Clustering: 50 Years Beyond K–Means [J]. Pattern recognition letters, 2010,1(8):651–666
[16] PIETRASZEK T, TANNER A. An Efficient K–Means with Good Initial Starting Points [J]. Georgian Electronic Scientific Journal: Computer Science and Telecommunications, 2009, 19(2):47–57
[17] SHEHROZ A A, KHAN S. Cluster Center Initialization Algorithm for K –Means Clustering[J]. Pattern Recognition Letters, 2004, 25(11): 1293–1302.doi: 10.1016/j.patrec.2004.04.007
[18] Stephen C H, REDMOND J. A Method for Initialising the K–Means Clustering Algorithm Using KD–Trees [J]. Pattern Recognition Letters, 2007, 28(8):965–973. doi: 10.1016/j.patrec.2007.01.001
[19] TAN P N, STEINBACH M, KUMAR V, et al. Introduction to Data Mining[J]. Pearson Addison Wesley Boston, 2006,1(1): 226–230
[20] ESTER M, KRIEGEL H P, SANDER J. A Density–Based Algorithm for Discovering Clusters in Large Spatial Databases with Noise [J]. Kdd,1996, 96: 226–231
[21] GENGeng J K, YE DAREN, LUO P. A Novel Algorithm DBCAPSIC for Clustering Non–Numeric Data[C] // To Appear the ACM SIGKDD Conference on Knowledge Discovery and Data Mining, Sydney, Australia, 2015

作者简介

杨曦，清华大学博士生；主要研究领域为软件可信性、软件工程理论与系统、数据库理论；先后主持和参加国家级基金项目5项，省部级项目10项；获得2项国家专利，发表论文10余篇。



GUL Jabeen，清华大学巴基斯坦籍博士生；主要研究领域为信息安全；已发表论文6篇，其中EI/SCI收录3篇。

罗平，清华大学教授；主要研究领域为网络空间安全；先后主持和参加国家级项目和国家科学基金项目20余项，获得教育部提名国家科学技术自然科学奖2等奖；已发表论文50余篇，其中被SCI检索30余篇。

⬅上接第13页

展，网络空间安全正面临着前所未有的发展机遇与挑战。通过分析传统线性结构防御体系以及传统的网络空间安全问题，结合当今严峻的新型网络空间安全威胁，我们提出一种新型立体式网络空间安全体系结构。新结构有助于实现立体式网络空间安全防域体系，并克服了传统线性防御体系只能应对单一性安全威胁的缺点。此外，我们还详细介绍了网络空间安全的基本范畴，并结合当前的热点应用，指出了立体式网络空间安全防御体系应采取的安全措施。

参考文献

[1] CLARK D D, WROCLAWSKI J, SOLLINS K R, et al. Tussle in Cyberspace: Defining Tomorrow's Internet [J]. IEEE/ACM Transactions on Networking, 2005, 13(3):462–475. doi: 10.1109/TNET.2005.850224
[2] 王晟, 虞红芳, 许都. 可信网络中安全、可控可管及可生存技术研究[J]. 中兴通讯技术, 2008, 14(1): 36–41
[3] NALEWAJSKI R F. Elements of Information Theory [J]. Perspectives in Electronic Structure Theory, 2011, 294(3–4): 371–395
[4] SCHWALM K T, SCHWALM K T. National Strategy to Secure Cyberspace [J]. Technical Report, AFRL–IF–RS–TR–2006–266, 2006, 1–27
[5] STEANE A M. How to Build a 300 bit, 1 Gop Quantum Computer [J]. Quantum Information & Computation, 2004, 7(3): 171–183
[6] 张阳, 陈开颜, 李雄伟,等. 基于差异度的密码芯片旁路攻击研究[J]. 通信学报, 2015, 3 (03): 100–105
[7] 唐科萍, 许方恒, 沈才樑. 基于位置服务的研究综述[J]. 计算机应用研究, 2012, 12(12): 4432–4436
[8] SINGH B, DHAWAN S, ARORA A, et al. A View of Cloud Computing[J]. Communications of the ACM, 2013, 53(4): 50–58
[9] 朱洪波, 杨龙祥, 于全. 物联网的技术思想与应用策略研究[J]. 通信学报, 2013, 5(5): 31–31
[10] ZHANG Y Q, WANG X Y. A Symmetric Image Encryption Algorithm Based on Mixed Linear–Nonlinear Coupled map Lattice [J]. Information Sciences, 2014, 273: 329–351
[11] 郑东, 赵庆兰, 张应辉. 密码学综述[J]. 西安邮电大学学报, 2013, 18(6): 1–10
[12] MANATHA G S, SHARMA S C. Network Layer Attacks and Defense Mechanisms in MANETS– A Survey [J]. International Journal of Computer Applications, 2010, 27 (1): 529–535
[13] ANDROULIDAKIS I. Mobile Phone Forensics [M]. Mobile Phone Security and Forensics. US: Springer, 2012: 75–99
[14] SHI Y, ZHENG Q, LIU J, et al. Directly

作者简介

张应辉，西安邮电大学通信与信息工程学院讲师、硕士生导师；主要研究方向为公钥密码学、云存储安全；目前主持国家自然科学基金；获得公开国家发明专利7项，其中授权2项，发表学术论文30余篇。

郑东，西安邮电大学通信与信息工程学院教授、博士生导师，西安邮电大学无线网络安全技术国家工程实验室主任；主要研究方向为基于编码的密码学、云存储安全；主持或参与了多项国家级研究课题，包括国家科技攻关项目、国家“863”计划项目等；出版学术专著2部，发表学术论文100余篇。

马春光，哈尔滨工程大学计算机学院教授、博士生导师；主要研究方向为信息安全与隐私保护、物联网等；主持完成了国家自然科学基金、教育部博士点基金等；获黑龙江省国防科技进步一等奖1项等，出版学术专著2部，发表学术论文60余篇。