4 云数据隐私度量的未来研究方向

上文依据 4 种类型总结了隐私度量方法的相关研究工作,但面向云数据的隐私度量的研究当前还处于发展初期,在云计算环境中还面临着诸多挑战.从现有的研究分析来看,未来云数据隐私度量的研究工作主要体现在隐私度量的过程、效果和方法 3 个方面.

4.1 隐私度量过程的研究

(1) 攻击者背景知识的动态、精准量化研究.为准确度量隐私信息泄露的程度,在设计隐私度量方法时需要充分考虑攻击者背景知识对隐私信息泄露的影响.这需要预测攻击者可能拥有的背景知识的具体内容和背景知识的量,已有的研究通常先假设攻击者可能拥有的背景知识,再利用关联规则等方法进行量化.事实上,假设的内容与攻击者的实际情况存在差异.因此,现有方法量化的背景知识与攻击者实际拥有的背景知识还存在差异.尤其是在云计算环境下,随着计算能力的提高,攻击者的背景知识和计算推理能力随时间变化飞速增长,对于背景知识随时间的变化而快速变化的动态、精准量化问题还有待进一步解决.

(2) 隐私保护强度与数据可用性之间的权衡研究.目前隐私保护方法需要牺牲数据可用性来获得较高的隐私保护强度,同时降低了云平台数据共享的服务质量.根据用户的实际情况分析隐私保护强度与云数据可用性的重要性,可以引用博弈论模型等方法在两者之间做出权衡.通过将博弈论与隐私度量相结合设计一种最优权衡的隐私保护度量机制,在给定能容忍的最大数据信息损失和计算开销的条件下,提供最优的隐私保护.如何权衡云数据可用性与有效保障用户隐私之间的关系亦是一个值得深入研究的问题.

4.2 隐私度量效果的研究

(1) 隐私度量粒度可控性研究.虽然现有的隐私度量方法能够实现依据不同隐私保护技术提供隐私度量,但在云服务中,同一云数据可能共享给多个数据使用者.因此,用户依据数据使用者的级别、数据的用途、不同时间段和安全级别等对云数据隐私度量的粒度需求均不相同.根据上述情况对云数据隐私度量进行细粒化处理,构造出结合这些因素变化的细粒度隐私度量方案是一个具有挑战性的问题.

(2) 隐私度量的效率优化研究.随着云计算、大数据技术在人们生活中的不断渗透,越来越多的数据外包到云服务提供商进行计算、共享、存储等.针对大规模多维的云数据产生速度快、流通量大等问题,如何提升云数据度量方法的效率、减少隐私度量的处理开销是云数据隐私度量方法可行性的关键.

4.3 隐私度量方法的研究

(1) 多种隐私度量方法的组合研究.面向云数据的隐私度量,由于用户拥有大量不同类型的数据,可能需要先进行聚类处理[66],再进行隐私度量;或这些数据可能经过不同的隐私保护方法进行处理,针对不同隐私保护方法的度量指标也不同,从而度量结果也不同,如匿名程度、信息熵值和差分隐私的隐私保护预算等,这可能需要融合多种隐私度量技术,如标准熵、标准互信息等.云计算环境中,针对已有的单一隐私度量方法存在的优缺点,有必要进一步对已有的隐私度量方法进行扩展和抽象,或者将多种隐私度量方法进行组合研究,进而设计出度量应用范围更广的隐私度量方法.

(2) 隐私度量的标准化研究.不同的云数据隐私度量方法能够度量不同隐私保护技术的隐私保护强度.现有的隐私度量方法主要建立在成熟隐私保护技术的基础上进行有针对性的度量.针对特定的隐私保护技术需要构建特定的隐私度量模型,不具备通用性且目前缺少一致的隐私度量标准,而隐私度量标准化可以减少可观察的特征,更容易定义和建模隐私度量.因此,设计一种标准化的云数据隐私度量模型,实现对不同类型的云数据隐私保护技术进行全面的、通用的隐私度量.

(3) 云数据全生命周期、动态演化的隐私度量研究.现有云服务已经渗透到人们日常生活的各个方面,然而,一旦采用云服务,数据的所有权与管理权分离,用户将会失去对数据的安全控制权.因此,从数据发布、存储、共享、使用到销毁的全生命周期各阶段均存在隐私信息泄露的风险[1].迫切需要引入隐私计算理论[67],结合云数据全生命周期和数据动态演化过程实施隐私度量.实现数据发布、存储、共享、使用、销毁的全生命周期各阶段

动态演化的隐私度量将对云数据隐私保护具有重要意义.

5 结束语

云服务为人们的生活提供了诸多便利,随之而来的云数据隐私保护问题不容小觑.目前,存在许多面向云数据的隐私保护技术,但如何有效评价面向云数据的隐私保护技术的可靠性依然是隐私保护领域面临的挑战性问题.其中,隐私保护强度是评估隐私保护技术的核心指标,研究隐私度量对隐私保护具有重大意义.本文主要对现有隐私度量方法的研究成果进行综述:首先,对隐私保护技术和隐私度量进行了概述,并给出了面向云数据的隐私保护技术性能评价指标和一种综合评价框架;然后,提出了一种面向云数据的隐私度量抽象模型,结合相关研究工作,对基于匿名的、基于信息熵的、基于集对分析理论和基于差分隐私这 4 类隐私度量方法的基本思想、实现原理等进行详细的分析、归纳和总结;最后分别总结了 4 类隐私度量方法主要的优缺点:基于匿名的隐私度量方法原理简单,可以结合攻击者及其背景知识进行度量,但该方法主要适用于匿名数据的度量;基于信息熵的隐私度量方法应用范围广,但度量结果易受异常值和错误数据等的影响;基于集对分析理论的隐私度量方法原理简单、应用范围广,但构建数据集之间的集对关系较复杂并未能结合攻击者及背景知识进行度量;基于差分隐私的隐私度量方法在数据元组独立时,无需考虑攻击者的背景知识,但其主要适用于加噪后的数据.最后,指出了面向云数据隐私度量的未来发展趋势.随着互联网以及新技术的发展,人们对信息隐私保护问题越来越关注,无论是理论研究还是在实际应用领域,隐私度量对隐私保护的研究都具有重大意义.从现有研究分析可知,当前面向云数据的隐私度量的研究还处于发展初期,隐私度量的研究与实际应用还需进一步研究与探索.

References:

[1] Xiong JB, Li FH, Liu XM, Yao ZQ, Chen P. A full lifecycle privacy protection scheme for sensitive data in cloud computing. Peer-to-Peer Networking and Applications, 2015,8(6):1025–1037. [doi: 10.1007/s12083-014-0295-x]

[2] Zhou SG, Li F, Tao YF, Xiao XK. Privacy preservation in database applications: A survey. Chinese Journal of Computes, 2009,32(5):847–858 (in Chinese with English abstract). [doi: 10.3724/SP.J.1016.2009.00847]

[3] Machanavajjhala A, Gehrke J. On the efficiency of checking perfect privacy. In: Proc. of the ACM SIGMOD-SIGACT-SIGART Symp. on Principles of Database. Chicago: ACM Press, 2006. 163–172. [doi: 10.1145/1142351.1142375]

[4] Liu YH, Zhang TY, Jin XL, Cheng XQ. Personal privacy protection in the era of big data. Journal of Computer Research and Development, 2015,52(1):229–247 (in Chinese with English abstract). [doi: 10.7544/issn1000-1239.2015.20131135]

[5] Mehmood A, Natgunanathan I, Xiang Y, Hua G, Guo S. Protection of big data privacy. IEEE Access on Theoretical Foundations for Big Data Applications, 2016,4:1821–1834. [doi: 10.1109/ACCESS.2016.2558446]

[6] Zhang X, Liu C, Nepal S, Yang C, Gou WC. A hybrid approach for scalable sub-tree anonymization over big data using MapReduce on cloud. Journal of Computer & System Science, 2014,80(5):1008–1020. [doi: 10.1016/j.jcss.2014.02.007]

[7] Mohammadian E, Noferesti M, Jalili R. FAST: Fast anonymization of big data streams. In: Proc. of the ACM Conf. on Big Data Science and Computing. Beijing: ACM Press, 2014. [doi: 10.1145/2640087.2644187]

[8] Yu JD, Dong X, Lou Y, Li ML. Differentially private wireless data publication in large-scale WLAN networks. In: Proc. of the IEEE Conf. on Parallel and Distributed Systems. Melbourne: IEEE Press, 2015. 290–297. [doi: 10.1109/ICPADS.2015.44]

[9] Li SD, Dou JW, Wang DS. Survey on homomorphic encryption and its applications to cloud security. Journal of Computer Research and Development, 2015,52(6):1378–1388 (in Chinese with English abstract). [doi: 10.7544/issn1000-1239.2015.20131494]

[10] Fun B, Wang K, Chen R, Yu P. Privacy-Preserving data publishing: A survey of recent development. ACM Computing Surveys, 2010,42(4):1–53. [doi: 10.1145/1749603.1749605]

[11] Bayardo RJ, Agrawal R. Data privacy through optimal *k*-anonymization. In: Proc. of the Int'l Conf. on Data Engineering. Washington: ACM Press, 2005. 217–228. [doi: 10.1109/ICDE.2005.42]

[12] Lu QW, Wang CM, Xiong Y. Personalized privacy-preserving trajectory data publishing. Chinese Journal of Electronics, 2017, 26(2):285–291 (in Chinese with English abstract). [doi: 10.1049/cje.2017.01.024]

[13] Xiao X, Tao Y. Personalized privacy preservation. In: Proc. of the ACM SIGMOD Int'l Conf. on Management of Data. Chicago: ACM Press, 2006. 229–240. [doi: 10.1145/1142473.1142500]

[14] Jiang HW, Zeng GS, Ma HY. Greedy clustering-anonymity method for privacy preservation of table data-publishing. Ruan Jian Xue Bao/Journal of Software, 2017,28(2):341–351 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/5015.htm [doi: 10.13328/j.cnki.jos.005015]

[15] Fun B, Wang K, Yu P. Top-Down specialization for information and privacy preservation. In: Proc. of the Int'l Conf. on Data Engineering. Tokoyo: ACM Press, 2005. 205–216. [doi: 10.1109/ICDE.2005.143]

[16] Gong QY, Yang M, Lou JZ. Data anonymization approach for microdata with relational and transaction attributes. Ruan Jian Xue Bao/Journal of Software, 2016,27(11):2828–2842 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/5099.htm [doi: 10.13328/j.cnki.jos.005099]

[17] Xiong JB, Yao ZQ, Ma JF, Liu XM, Li Q, Ma J. PRIAM: Privacy preserving identity and access management scheme in cloud. KSII Trans. on Internet and Information Systems, 2014,8(1):282–304. [doi: 10.11959/j.issn.1000-436x.2016176]

[18] Chen BC, Ramakrishnan R, Lefevre K. Privacy skyline: Privacy with multidimensional adversarial knowledge. In: Proc. of the Int'l Conf. on Very large Data Bases. Vienna: ACM Press, 2007. 770–781.

[19] Li TC, Li NH. Injector: Mining background knowledge for data anonymization. In: Proc. of the Int'l Conf. on Data Engineering. NewYork: ACM Press, 2008. 446–455.

[20] Cai ZP, He Z, Guan X, Li YS. Collective data-sanitization for preventing sensitive information inference attacks in social networks. IEEE Trans. on Dependable and Secure Computing, 2016,(99):1–14. [doi: 10.1109/TDSC.2016.2613521]

[21] Du W, Teng Z, Zhu Z. Privacy-MaxEnt: Integrating background knowledge in privacy quantification. In: Proc. of the ACM SIGMOD Int'l Conf. on Management of Data. Vancouver, 2008. 459–472.

[22] Wang CM, Gou YJ, Gou YH. Privacy metric for user's trajectory in location-based services. Ruan Jian Xue Bao/Journal of Software, 2012,23(2):352–360 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/3946.htm [doi: 10.3724/SP.J.1001.2012.03946]

[23] Li T, Li NH, Zhang J. Modeling and integrating background knowledge in data anonymization. In: Proc. of the IEEE Int'l Conf. on Data Engineering. Shanghai, 2009. 6–17. [doi: 10.1109/ICDE.2009.86]

[24] Mao YX, Chen TB, Shi BL. Efficient method for mining multiple-level and generalized association rules. Ruan Jian Xue Bao/Journal of Software, 2011,22(12):2965–2980 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/3907.htm [doi: 10.3724/SP.J.1001.2011.03907]

[25] Sweeney L. *k*-Anonymity: A model for protecting privacy. Int'l Journal on Uncertainty, Fuzziness and Knowledge-Based Systems, 2002,10(5):557–570.

[26] Machanavajjhala A, Gehrke J, Kifer D. *l*-Diversity: Privacy beyond *k*-anonymity. In: Proc. of the IEEE Int'l Conf. on Data Engineering. Atlanta: IEEE Press, 2006. 24–35.

[27] Li NH, Li TC, Venkata S. *t*-Closeness: Privacy beyond *k*-anonymity and *l*-diversity. In: Proc. of the IEEE Int'l Conf. on Data Engineering. Istanbul: IEEE Press, 2007. 106–115. [doi: 10.1103/ICDE.2007.367856]

[28] Li NH, Li TC, Nkatasubramanian S. (*n*,*t*)-Closeness: A new privacy measure for date publishing. IEEE Trans. on Knowledge and Date Engineering, 2010,22(7):943–956. [doi: 10.1109/TKDE.2009.139]

[29] Zhang JP, Xie J, Yang J, Zhang B. A *t*-closeness privacy model based on sensitive attribute values semantics bucketization. Journal of Computer Research and Development, 2014,51(1):126–137 (in Chinese with English abstract). [doi:10.7544/issn1000-1239.2014.20130688]

[30] Gkountouna O, Terrovitis M. Anonymizing collections of tree-structured data. IEEE Trans. on Knowledge and Data Engineering, 2015,27(8):2034–2048.

[31] Yuji Y, Kouichi I. *k*-Presence-Secrecy: Practical privacy model as extension of *k*-anonymity. IEICE Trans. on Information & System, 2017,(4):730–740. [doi: 10.1587/transinf.2016DA0015]

[32] Li XY, Zhang CH, Jung T, Qian JW, Chen LL. Graph-Based privacy-preserving data publication. In: Proc. of the IEEE Int'l Conf. on Computer Communications. San Francisco: IEEE Press, 2016. 1–9. [doi: 10.1109/INFOCOM.2016.7524584]

[33] Shannon C. A mathematical theory of communication. The Bell System Technical Journal, 1948,27(3):379–423.

[34] Clauß S, Stefan S. Structuring anonymity metrics. In: Proc. of the ACM Conf. on Computer and Communications Security. Alexandria: ACM Press, 2006. 55–62.

[35] Peng CG, Ding HF, Zhu YJ, Tian YL, Fu ZF. Information entropy models and privacy metrics methods for privacy protection. Ruan Jian Xue Bao/Journal of Software, 2016,27(8):1891–1903 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/5096.htm [doi: 10.13328/j.cnki.jos.005096]

[36] Zhang HL, Shi YL, Zhang SD, Zhou ZM, Cui LZ. A privacy protection mechanism for dynamic data based on partition-confusion. Journal of Computer Research and Development, 2016,53(11):2454–2464 (in Chinese with English abstract). [doi: 10.7544/issn1000-1239.2016.20150553]

[37] Diaz C, Troncoso C, Danezis G. Does additional information always reduce anonymity. In: Proc. of the ACM Workshop on Privacy in the Electronic Society. Alexandria: ACM Press, 2007. 72–75.

[38] Lai LF, Ho SW, Poor HV. Privacy-Security trade-offs in biometric security systems. Part II: Multiple use case. IEEE Trans. on Information Forensics & Security, 2011,6(1):140–151. [doi: 10.1109/TIFS.2010.2098872]

[39] Asoodeh S, Alajaji F, Linder T. Notes on information-theoretic privacy. In: Proc. of the IEEE Conf. on Communication, Control and Computing. Monticello: IEEE Press, 2015. 1272–1278.

[40] Calmon F, Makhdoumi A, Médard M. Fundamental limits of perfect privacy. In: Proc. of the IEEE Int'l Symp. on Information Theory. HongKong: IEEE Press, 2015. 1796–1800.

[41] Alvim M, Andrés M, Chatzikokolakis K, Pierpaolo D, Palamidessi C. On the information leakage of differentially-private mechanisms. Journal of Computer Security, 2015,23(4):427–469.

[42] Calmon F, Fawaz N. Privacy against statistical inference. In: Proc. of the IEEE Conf. on Communication, Control and Computing. Monticello: IEEE Press, 2012. 1401–1408.

[43] Humbert M, Ayday E, Hubaux JP, Telenti A. Addressing the concerns of the lacks family: Quantification of kin genomic privacy. In: Proc. of the ACM Conf. on Computer and Communications Security. Berlin: ACM Press, 2013. 1141–1152. [doi: 10.1145/2508859.2516707]

[44] Humbert M, Ermanayda Y, Hubaux JP, Telenti A. Quantifying interdependent risks in genomic privacy. ACM Trans. on Privacy & Security, 2017,20(1):1–30. [doi: 10.1145/3035538]

[45] Zhao KQ. Disposal and description of uncertainties based on the set pair analysis. Information and Control, 1995,24(3):162–166 (in Chinese with English abstract). [doi: 10.13976/j.cnki.xk.1995.03.006]

[46] Yan Y, Hao XH, Wang WJ. A set pair analysis method for privacy metric. Engineering Journal of Wuhan University, 2015,48(6):883–890 (in Chinese with English abstract). [doi: 10.14188/j.1671-8844.2015-06-027]

[47] Dwork C. Differential privacy. In: Proc. of the Int'l Colloquium on Automata, Languages and Programming. Berlin: Springer-Verlag, 2006. 1–12. [doi: 10.1007/11787006_1]

[48] Dwork C, Lei J. Differential privacy and robust statistics. In: Proc. of the ACM Symp. on Theory of Computing. Bethesda: ACM Press, 2009. 371–380.

[49] Dwork C, Mcsherry F, Nissim K, Smith A. Calibrating noise to sensitivity in private data analysis. Theory of Cryptography, 2006,7(8):265–284. [doi: 10.1007/11681878_14]

[50] Chen R, Acs G, Castelluccia C. Differential private sequential data publication via variable-length *N*-grams. In: Proc. of the ACM Conf. on Computer and Communication Security. Raleigh: ACM Press, 2012. 638–649.

[51] Zhang WJ, Li H. A differentially-private mechanism for multi-level data publishing. Chinese Journal of Network and Information Security, 2015,1(1):58–65 (in Chinese with English abstract). [doi: 10.11959/j.issn.2096-109x.2015.00008]

[52] Jorgensen Z, Yu T, Cormode G. Conservative or liberal? Personalized differential privacy. In: Proc. of the IEEE Int'l Conf. on Data Engineering. Seoul: IEEE Press, 2015. 1023–1034. [doi: 10.1109/ICDE.2015.7113353]

[53] Chen R, Fung BCM, Yu P, Desai B. Correlated network data publication via differential privacy. The Int'l Journal on Very Large Data Bases, 2014,23(4):653–676.

[54] Kifer D, Machanavajjhala A. Pufferfish: A framework for mathematical privacy definitions. ACM Trans. on Database Systems, 2014,39(1):671–683.

[55] Yang B, Sato I, Nakagawa H. Bayesian differential privacy on correlated data. In: Proc. of the ACM SIGMOD Int'l Conf. on Management of Data. Melbourne: ACM Press, 2015. 747–762. [doi: 10.1145/2723372.2747643]

[56] Zhu TQ, Xiong P, Li G, Zhou W. Correlated differential privacy: Hiding information in non-IID data set. IEEE Trans. on Information Forensics and Security, 2015,10(2):229–242. [doi: 10.1109/TIFS.2014.2368363]

[57] Wu XT, Dou WC, Ni Q. Game theory based privacy preserving analysis in correlated data publication. In: Proc. of the Australasian Computer Science Week Multi-Conf. Geelong: ACM Press, 2017. 73–82. [doi: 10.1145/3014812.3014887]

[58] Barthe G, Kopf B. Information-Theoretic bounds for differentially private mechanisms. In: Proc. of the Computer Security Foundations Symp. Washington: IEEE Press, 2011. 191–204.

[59] Alvim M, Andres M, Chatzikokolakis K, Degano P, Palamidessi C. Differential privacy: On the trade-off between utility and information leakage. In: Proc. of the Int'l Conf. on Formal Aspects of Security and Trust. Leuven: ACM Press, 2012. 39–54.

[60] Wang W, Ying L, Zhang J. On the relation between identifiability, differential privacy, and mutual-information privacy. IEEE Trans. on Information Theory, 2016,62(9):5018–5029. [doi: 10.1109/TIT.2016.2584610]

[61] Cuff P, Yu LQ. Differential privacy as a mutual information constraint. In: Proc. of the ACM SIGSAC Conf. on Computer and Communications Security. Vienna: ACM Press, 2016. 43–54. [doi: 10.1145/2976749.2978308]

[62] Wagner I, Eckhoff D. Technical privacy metrics: A systematic survey. arXiv Preprint arXiv:1512.00327, 2015.

[63] Wan S, Li FH, Niu B,Sun Z, Li H. Research progress on location privacy-preserving techniques. Journal on Communications, 2016,37(12):124–141 (in Chinese with English abstract). [doi: 10.11959/j.issn.1000-436x.2016279]

[64] Toth G, Hornak Z, Vajda F. Measuring anonymity revisited. In: Proc. of the NORDIC Workshop on Secure IT Systems. Helsinki: ACM Press, 2004. 85–90.

[65] Murdoch S. Quantifying and measuring anonymity. In: Data Privacy Management and Autonomous Spontaneous. Berlin: Springer-Verlag, 2014. 3–13. [doi: 10.1007/978-3-642-54568-9_1]

[66] Wu DP, Yang BR, Wang HG, Wang CB, Wang RY. Privacy-Preserving multimedia big data aggregation in large-scale wireless sensor networks. ACM Trans. on Multimedia Computing, Communications and Applications, 2016,12(4). [doi: 10.1145/2978570]

[67] Li FH, Li H, Jia Y, Yu NH, Weng J. Privacy computing: Concept, connotation and its research trend. Journal on Communications, 2016,37(4):1–11 (in Chinese with English abstract).

附中文参考文献:

[2] 周水庚,李丰,陶宇飞,肖小奎.面向数据库应用的隐私保护研究综述.计算机学报,2009,32(5):847–858. [doi: 10.3724/SP.J.1016.2009.00847]

[4] 刘雅辉,张铁赢,靳小龙,程学旗.大数据时代的个人隐私保护.计算机研究与发展,2015,52(1):229–247. [doi: 10.7544/issn1000-1239.2015.20131135]

[9] 李顺东,窦家维,王道顺.同态加密算法及其在云安全中的应用.计算机研究与发展,2015,52(6):1378–1388. [doi: 10.7544/issn1000-1239.2015.20131494]

[14] 姜火文,曾国荪,马海英.面向表数据发布隐私保护的贪心聚类匿名方法.软件学报,2017,28(2):341–351. http://www.jos.org.cn/1000-9825/5015.htm [doi: 10.13328/j.cnki.jos.005015]

[16] 龚奇源,杨明,罗军舟.面向关系-事务数据的数据匿名方法.软件学报,2016,27(11):2828–2842. http://www.jos.org.cn/1000-9825/5099.htm [doi:10.13328/j.cnki.jos.005099]

[22] 王彩梅,郭亚军,郭艳华.位置服务中用户轨迹的隐私度量.软件学报,2012,23(2):352–360. http://www.jos.org.cn/1000-9825/3946.htm [doi:10.3724/SP.J.1001.2012.03946]

[24] 毛宇星,陈彤兵,施伯乐.一种高效的多层和概化关联规则挖掘方法.软件学报,2011,22(12):2965–2980. http://www.jos.org.cn/1000-9825/3907.htm [doi:10.3724/SP.J.1001.2011.03907]

[29] 张健沛,谢静,杨静,张冰.基于敏感属性值语义桶分组的 *t*-closeness 隐私模型.计算机研究与发展,2014,51(1):126–137. [doi: 10.7544/issn1000-1239.2014.20130688]

[35] 彭长根,丁红发,朱义杰,田有亮,符祖峰.隐私保护的信息熵模型及其度量方法.软件学报,2016,27(8):1891–1903. http://www.jos.org.cn/1000-9825/5096.htm [doi: 10.13328/j.cnki.jos.005096]

[36] 张宏磊,史玉良,张世栋,周中民,崔立真.一种基于分块混淆的动态数据隐私保护机制.计算机研究与发展,2016,53(11):2454–2464. [doi: 10.7544/issn1000-1239.2016.20150553]

[45] 赵克勤.集对分析对不确定性的描述和处理.信息与控制,1995,24(3):162–166. [doi: 10.13976/j.cnki.xk.1995.03.006]

[46] 晏燕,郝晓弘,王万军.一种隐私保护度量的集对分析方法.武汉大学学报,2015,48(6):883–890. [doi: 10.14188/j.1671-8844.2015-06-027]

[51] 张文静,李晖.差分隐私保护下的数据分级发布机制.网络与信息安全学报,2015,1(1):58–65. [doi: 10.11959/j.issn.2096-109x.2015.00008]

[63] 万盛,李凤华,牛犇,孙哲,李晖.位置隐私保护技术研究进展.通信学报,2016,37(12):124–141. [doi: 10.11959/j.issn.1000-436x.2016279]

[67] 李凤华,李晖,贾焰,俞能海,翁健.隐私计算研究范畴及发展趋势.通信学报,2016,37(4):1–11. [doi: 10.11959/j.issn.1000-436x.2016078]

熊金波(1981－),男,湖南益阳人,博士,副教授,CCF 专业会员,主要研究领域为云数据安全,隐私保护技术.

马蓉(1992－),女,硕士生,CCF 学生会员,主要研究领域为云数据安全,隐私保护技术.

王敏燊(1994－),男,硕士生,CCF 学生会员,主要研究领域为信任评估,数据安全.

姚志强(1967－),男,博士,教授,CCF 高级会员,主要研究领域为信息安全.

田有亮(1982－),男,博士,教授,博士生导师,主要研究领域为算法博弈论,数据安全,隐私保护.

林铭炜(1985－),男,博士,副教授,CCF 专业会员,主要研究领域为存储系统,嵌入式系统.