Jaideep S. Vaidya

Management Science and Information Systems Department
Rutgers University
180 University Avenue
Newark, NJ 07102-1803
(973)353-1441
http://cimic.rutgers.edu/~jsvaidya

41 River Road
East Brunswick, NJ 08816
H-1B Visa

Email: jsvaidya@rbs.rutgers.edu

Research Interests

I am primarily interested in the idea of secure information sharing and its various applications. My research contributions lie primarily in the field of Security or the field of Data Mining, or most successfully, at the interoperation of the two. The confluence of Privacy/Security, Data Mining and Databases leads to very interesting research issues. As such, I am interested in security and privacy issues raised by data mining; as also the application of secure computation technologies to business processes such as supply chain management and optimization. Other areas of interest include the application of data mining techniques to interoperation of heterogeneous information sources as well as the use of data mining for enhancing security.

Education

Purdue University *West Lafayette, Indiana, USA*

Ph.D., Computer Science, August 2004

- Dissertation Topic: "Privacy Preserving Data Mining over Vertically Partitioned Data"
  Privacy and security concerns can prevent sharing of data, derailing data mining projects. Distributed knowledge discovery, if done correctly, can alleviate this problem. The key is to obtain valid results, while providing guarantees on the (non)disclosure of data. We focus on vertically partitioned data: situations where different sites contain different attributes for a common set of entities. The key challenges are to propose provably secure solutions that are also practical. The thesis argues that it is indeed possible to have *efficient* and *practical* techniques for provably privacy-preserving mining of knowledge from large amounts of data. The dissertation presents several privacy preserving data mining algorithms operating over vertically partitioned data. The set of underlying techniques solving independent sub-problems are also presented. Together, these enable the secure "mining" of knowledge.
- Advisor: Chris Clifton

M.S., Computer Science, May 2001

Mumbai University *Mumbai, Maharashtra, India*

B.S., Computer Engineering, May, 1999

- Term Project: Implemented in C, a Text to Speech Synthesis system for the Indian National Language, Hindi, in collaboration with Faculte Polytechnic de Mons, Belgium. Received a Special Commendation from the Principal of the College.

Professional Experience

Rutgers, the State University of New Jersey **August, 2004 – present**
Assistant Professor of Computer Information Systems. Research in data mining, databases and security. Teaching: Management Information Systems, Introduction to Software Development, Computer Information Systems, Information Systems Analysis, Information Systems Design, Structured Programming Applications, Business Applications Programming.

Purdue University **August, 1999 – June, 2004**
Research Assistant in the Department of Computer Sciences (affiliated with CERIAS and ICDS).

Teaching Assistant for *Computer Architecture, Compilers: Principles and Practice and graduate level Cryptography*. Work involved instructing recitation sessions, grading and assisting students.

NEC C&C Research Labs **May, 2002 – August, 2002**
Summer Intern as part of the Content Aware Networks group. Work on security issues in content aware networks. Mentor: Wen-Syan Li

Microsoft Corporation **May, 2000 – August, 2000**
Summer Intern as part of the Trident Team in the Internet Explorer Group. Core responsibility was to add W3C Document Object Model (DOM) Level 1 support to IE 6.0.

Honors and Awards

1. NSF Career Award, 2008
2. Listed in Marquis Who's Who, 2006
3. Best Industrial Paper award at IEEE ICDE '05
4. Honorable Mention (runner up), best research paper at ACM SIGKDD '03
5. Member of Upsilon Pi Epsilon, the CS Honor Society
6. AAAI and SIGMOD Student Scholarship (Travel Award for KDD '03)
7. State Merit Scholarships awarded by the state of U.P. (1989) and Maharashtra (1990), India

Monograph

1. "Privacy Preserving Data Mining". Jaideep Vaidya, Michael Zhu and Chris Clifton, Monograph, Series on Advances in Information Security, Springer-Verlag, November 2005, ISBN: 0-387-25886-8.

Book Chapters

1. "A Survey of Privacy-Preserving Methods across Vertically Partitioned Data", Jaideep Vaidya in *Privacy-Preserving Data Mining: Models and Algorithms*, Charu Aggarwal, Philip S. Yu, eds., Springer, 2008.
2. "Privacy, Profiling, Targeted Marketing, and Data Mining", Jaideep Vaidya and Vijay Atluri in *Digital Privacy: Theory, Technologies, and Practices*, A. Acquisti, S. Gritzalis, C. Lambrinoudakis, S. di Vimercati, eds., Taylor and Francis, December 18, 2007.
3. "Defining Privacy for Data Mining". Book Chapter. Chris Clifton, Murat Kantarcioglu and Jaideep Vaidya in *Data Mining: Next Generation Challenges and Future Directions*, AAAI/MIT Press, October 1, 2004.
4. "Privacy-Preserving Data Mining". Chris Clifton, Murat Kantarcioglu and and Jaideep Vaidya, invited chapter in *Foundations and Advances in Data Mining Computing*, T.Y. Lin and Wesley Chu, eds., Springer-Verlag, October 2005.

Journal Articles

1. "Efficient Security Policy Enforcement for the Mobile Environment", Vijayalakshmi Atluri, Heechang Shin, and Jaideep Vaidya, accepted for publication in Journal of Computer Security, IOS Press, NL.
2. "Privacy Preserving SVM Classification", Jaideep Vaidya, Hwanjo Yu and Xiaoqian Jiang, in Knowledge and Information Systems, Springer-Verlag, 14(2), pp. 161-178, February, 2008.
3. "An Approach to Identifying Beneficial Collaboration Securely in Decentralized Logistics Systems". Chris Clifton, Ananth Iyer, Richard Cho, Wei Jiang, Murat Kantarcioglu and Jaideep Vaidya, Manufacturing & Service Operations Management, 10(1), Winter 2008, pp. 108 – 125, INFORMS, Linthicum, Maryland.

4. "Privacy Preserving Naïve Bayes Classification". Jaideep Vaidya, Murat Kantarcioglu and Chris Clifton, accepted for publication in the International Journal on Very Large Data Bases, Springer-Verlag, GmbH.
5. "Secure Set Intersection Cardinality with Application to Association Rule Mining". Jaideep Vaidya and Chris Clifton, Journal of Computer Security, 13(4), IOS Press, November 2005, pp. 593 - 622.
6. "Privacy-Preserving Data Mining: Why, How, and When?". Jaideep Vaidya and Chris Clifton, IEEE Security & Privacy, New York, NY, November/December 2004.

Under Review

1. "Privacy Preserving Linear SVM Classification". Hwanjo Yu and Jaideep Vaidya, submitted (September 2004) to Data & Knowledge Engineering, Elsevier Science, Amsterdam. 2nd review.
2. "Role Engineering via Prioritized Subset Enumeration", Jaideep Vaidya, Vijayalakshmi Atluri, and Janice Warner, submitted (December 2006) to IEEE Transactions on Dependable and Secure Computing.
3. "Privacy-Preserving Top-K Queries", Jaideep Vaidya and Chris Clifton, submitted (March 2007) to IEEE Transactions on Knowledge and Data Engineering, IEEE Computer Society. 2nd review.
4. "Role Engineering for Minimizing Administrative Assignments", Jaideep Vaidya, Vijayalakshmi Atluri, Qi Guo, and Haibing Lu, submitted (September 2007) to Journal of Computer Security, IOS Press, NL.
5. "Privacy-Preserving Decision Trees over Vertically Partitioned Data". Jaideep Vaidya, Chris Clifton, Murat Kantarcioglu and A. Scott Patterson, submitted (September 2007) to ACM Transactions on Knowledge Discovery in Data, ACM.
6. "Exploring the Benefits of Information Sharing in a Distribution System", Xiaolong Zhang, Yao Zhao and Jaideep Vaidya, submitted (November 2007) to European Journal of Operational Research, Elsevier.
7. "Privacy Preserving Indexing of Documents". Mayank Bawa, Rakesh Agrawal, Roberto J. Bayardo and Jaideep Vaidya, submitted (December 2007) to the International Journal on Very Large Data Bases, Springer.
8. "Towards a United Index Structure for Spatiotemporal Data and Authorizations", Vijayalakshmi Atluri, Qi Guo, Heechang Shin, and Jaideep Vaidya, submitted (January 2008) to the ACM Transactions on Database Systems.

Refereed Conference and Workshop Papers

1. "Migrating to Optimal RBAC with Minimal Perturbation", Jaideep Vaidya, Vijayalakshmi Atluri, Qi Guo, and Nabil Adam, in Proceedings of the 13th ACM Symposium on Access Control Models and Technologies (SACMAT), June 11-13, 2008, Estes Park, Colorado, USA.
2. "Secure Information Sharing and Analysis for Effective Emergency Management", Nabil Adam, Vijayalakshmi Atluri, Soon Ae Chun, John Ellenberger, Basit Shafiq, Jaideep Vaidya, and Hui Xiong, in Proceedings of the 9th Annual International Conference on Digital Government Research, May 18-21, 2008, Montreal, Canada.
3. "A Profile Anonymization Model for Privacy in a Personalized Location Based Service Environment", Heechang Shin, Vijayalakshmi Atluri, and Jaideep Vaidya, in Proceedings of the 9th International Conference on Mobile Data Management, April 27-30, 2008, Beijing, China.
4. "Privacy-preserving Link Discovery", Xiaoyun He, Basit Shafiq, Jaideep Vaidya, and Nabil Adam, in Proceedings of the 23rd Annual ACM Symposium on Applied Computing, Data Mining Track, March 16-20, 2008, Fortaleza, Ceara, Brazil.

5. "Optimal Boolean Matrix Decomposition: Application to Role Engineering", Haibing Lu, Jaideep Vaidya, and Vijay Atluri, in Proceedings of the 24th International Conference on Data Engineering, April 7-12, 2008, Cancun, Mexico.
6. "Privacy Preserving Integration of Health Care Data", Nabil Adam, Thomas White, Basit Shafiq, Jaideep Vaidya, and Xiaoyun He, American Medical Informatics Association 2007 Annual Symposium, November 10-14, 2007, Chicago, Illinois.
7. "Enabling better Medical Image Classification through Secure Collaboration", Jaideep Vaidya and Bhakti Tulpule, in Proceedings of the 14th IEEE International Conference on Image Processing, September 16-19, 2007, San Antonio, Texas.
8. "The Role Mining Problem: Finding a Minimal Descriptive Set of Roles", Jaideep Vaidya, Vijay Atluri, and Qi Guo, in Proceedings of the 12th ACM Symposium on Access Control Models and Technologies, June 20-June 22, 2007, Sophia Antipolis, France.
9. "Collaboration Based Access Control Using Semantics", Janice Warner, Vijay Atluri, Ravi Mukkamala and Jaideep Vaidya, in Proceedings of the 12th ACM Symposium on Access Control Models and Technologies, June 20-June 22, 2007, Sophia Antipolis, France.
10. "RoleMiner: Finding Roles using Subset Enumeration", Jaideep Vaidya, Vijay Atluri, and Janice Warner, in Proceedings of the 13th ACM Conference on Computer and Communications Security, October 30-November 3, Alexandria, VA, USA.
11. "Privacy-Preserving SVM Classification on Vertically Partitioned Data", Hwanjo Yu, Jaideep Vaidya and Xiaoqian Jiang, in Proceedings of the 10th Pacific-Asia conference on Knowledge Discovery and Data Mining, April 9-12, Singapore.
12. "Privacy-Preserving SVM using Nonlinear Kernels on Horizontally Partitioned Data", Hwanjo Yu, Xiaoqian Jiang and Jaideep Vaidya, in the 21st Annual ACM Symposium on Applied Computing, Data Mining Track, April 23-27, 2006, Dijon, France.
13. "Privacy Preserving Decision Tree Classification for vertically partitioned data", Jaideep Vaidya and Chris Clifton, in the proceedings of the Nineteenth Annual IFIP WG 11.3 Working Conference on Data and Applications Security, August 7-10, 2005, Storrs, CT.
14. "Collusion Set Detection through Outlier Discovery", Vandana Janeja, Vijay Atluri, Jaideep Vaidya and Nabil R. Adam, IEEE International Conference on Intelligence and Security Informatics, May 19-20, 2005, Atlanta, GA.
15. "Knowledge Discovery from Transportation Network Data". Wei Jiang, Jaideep Vaidya, Zahir Balaporia, Chris Clifton, and Brett Banich, in proceedings of the Twenty First IEEE International Conference on Data Engineering, April 5-8, 2005, Tokyo, Japan. Best Industrial Paper award.
16. "Privacy Preserving Top-K Queries". Jaideep Vaidya and Chris Clifton, in proceedings of the Twenty First IEEE International Conference on Data Engineering, April 5-8, 2005, Tokyo, Japan.
17. "Privacy Preserving Outlier Detection". Jaideep Vaidya and Chris Clifton, in proceedings of the Fourth IEEE International Conference on Data Mining, November 1-4, 2004, Brighton, UK.
18. "Privacy Preserving Data Integration and Sharing". Chris Clifton, AnHai Doan, Ahmed Elmagarmid, Murat Kantarcioglu, Gunther Schadow, Dan Suciu, and Jaideep Vaidya, The 9th ACM SIGMOD Workshop on Research Issues in Data Mining and Knowledge Discovery (DMKD'2004) June 13, 2004, Paris, France.
19. "Privacy Preserving Naïve Bayes Classifier for Vertically Partitioned Data". Jaideep Vaidya and Chris Clifton, in the Proceedings of the 2004 SIAM International Conference on Data Mining, April 22-24, 2004, Lake Buena Vista, Florida, USA.
20. "Privacy Preserving Naive Bayes Classifier for Horizontally Partitioned Data". Murat Kantarcioglu and Jaideep Vaidya, in the 2^{nd} Workshop on Privacy Preserving Data Mining held in association with The Third IEEE International Conference on Data Mining, November 19 - 22, 2003, Melbourne, FL.

21. "Leveraging the "Multi" in Secure Multi-Party Computation". Jaideep Vaidya and Chris Clifton, in the Workshop on Privacy in the Electronic Society held in association with The Tenth ACM Conference on Computer and Communications Security, October 27 - 31, 2003, Washington, D.C.
22. "Privacy-Preserving K-Means Clustering over Vertically Partitioned Data". Jaideep Vaidya and Chris Clifton, The Ninth ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, August 24 - 27, 2003, Washington, D.C. Honorable mention (runner up), best research paper.
(Revised paper invited for submission at Interface '04).
23. "Privacy Preserving Association Rule Mining in Vertically Partitioned Data". Jaideep Vaidya and Chris Clifton, The Eighth ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, July 23 - 26, 2002, Edmonton, Alberta, Canada.
24. "An architecture for Privacy-preserving Mining of Client Information". Murat Kantarcioglu and Jaideep Vaidya, in Volume 14 - Privacy, Security and Data Mining of the ACS Series Conferences in Research and Practice in Information Technology.

Editor Refereed Articles

1. "Using Secure-coprocessor for creating efficient Privacy-Preserving Distributed Data Mining Toolbox". Murat Kantarcioglu, Jaideep Vaidya and Chris Clifton, in International Workshop on Privacy and Security Issues in Data Mining held in conjuction with ECML/PKDD 2004, September 20, 2004, Italy. Invited paper.
2. "Tools for Privacy Preserving Distributed Data Mining". Chris Clifton, Murat Kantarcioglu, Jaideep Vaidya, Xiaodong Lin and Michael Zhu, in ACM SIGKDD Explorations 4(2), December 2002. Invited paper.
3. "Defining Privacy for Data Mining". Chris Clifton, Murat Kantarcioglu and Jaideep Vaidya, in Proceedings of the National Science Foundation Workshop on Next Generation Data Mining, November 1-3, 2002, Baltimore, MD. Invited paper.

Research Funding

- Co-Principal Investigator, "DG: Secure Agency Interoperation for Effective Data Mining in Border Control and Homeland Security Applications", Supplement, $50,000, NSF. (Nabil R. Adam, PI).
- Principal Investigator, "Collaborative Optimization with Limited Information Disclosure", $450,000, NSF Career Award 2008, February 2008 - January 2013 (No Co-PIs).
- Co-Principal Investigator, "Improving Business Knowledge Management & Analysis Through the use of the RFID Technology and Semantic Web Services", $566,000, SAP Corporation, August 2007 - June 2009.
- Internal Grant: Co-Principal Investigator, "Information Technology for Emergency Management (iTeam)", $40,000, Rutgers Academic Excellence Fund, 2007-2008. (Nabil R. Adam, PI).
- Internal Grant: Principal Investigator, "Privacy Preserving Optimization", Rutgers FOM Research Grant, $1,500, July 2006 - June 2007.
- Internal Grant: Principal Investigator, "Privacy Preserving Data Analysis", Rutgers FOM Research Grant, $9,500, July 2005 - June 2006.
- Co-Principal Investigator, "Improving Business Knowledge Management and Analysis Through the use of Semantic Web Services and RFID Technology", SAP Research Labs, $420,000, June 2004 - June 2007. (Nabil R. Adam, PI).

Presentations

1. Role Engineering and the Role Mining Problem, University of Texas at Dallas, Dallas, TX, September 17, 2007.
2. Role Engineering and the Role Mining Problem, Tata Research Design & Development Center, August 1, 2007, Pune, India.
3. "RoleMiner: Role Mining via Subset Enumeration", at the 13th ACM Conference on Computer and Communications Security, November 1, 2006.
4. "Privacy-Preserving Data Mining", at the Tata Research Design & Development Center, Pune, India, June 21, 2005.
5. "Privacy-Preserving Outlier Detection", at the Stevens Institute of Technology, Hoboken, NJ, May 2, 2005.
6. "Privacy Preserving Collaboration – Supply Chain, Transportation Logistics and Other problems", Supply Chain Management Research Seminar Series, Rutgers Business School, April 28, 2005.
7. "Privacy Preserving K-Means Clustering on Vertically Partitioned Data", invited talk at Interface '04, the best of data mining at KDD session, Baltimore, Maryland, May 27, 2004.
8. "Privacy Preserving Data Mining over Vertically Partitioned Data" at the CSIS Seminar at the Department of Information and Software Engineering, George Mason University, May 25, 2004.
9. "Privacy Preserving Data Mining on Vertically Partitioned Data" at the CERIAS Security Seminar, Purdue University, January 14, 2004.
10. "Privacy Preserving Data Mining over Vertically Partitioned Data" at the DAIS Seminar at the CS Department at University of Illinois at Urbana-Champaign, October 24, 2003.
11. "Leveraging the "Multi" in Secure Multi-Party Computation" at the Workshop on Privacy in Electronic Society held in conjunction with ACM CCS, October 30, 2003.
12. "Privacy Preserving K-Means Clustering over Vertically Partitioned Data" at the Ninth ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, August 25, 2003.
13. "A new architecture for Privacy Preserving Data Mining" at the Workshop on Privacy, Security and Data Mining held in conjunction with ICDM, December 9, 2002.
14. "Privacy Preserving Data Mining" with Chris Clifton in CERIAS Security Seminar, February 27, 2002.
15. "A new architecture for Privacy Preserving Data Mining" in Indiana Center for Database Systems seminar, December 4, 2002.

Professional Activities

Publicity Chair

- 2008 Workshop on Secure Knowledge Management, November 3-4, 2008, Richardson, TX, USA.

Co-Program Chair

- 6th International Workshop on Privacy Aspects of Data Mining, held in conjunction with the 2007 IEEE International Conference on Data Mining, October 28, 2007, Omaha, NE, USA.

Proceedings Chair

- The Eleventh ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, August 21-24, 2005, Chicago, IL.

Book Donations Chair

- ACM SIGMOD/PODS 2005 Conference, June 14-16, 2005, Baltimore, MD.

Program Committee

- 2008 Workshop on Secure Knowledge Management, November 3-4, 2008, Richardson, TX, USA.
- 2008 IEEE International Conference on Granular Computing, August 26-28, 2008, Hangzhou, China.
- 10th International Conference on Data Warehousing and Knowledge Discovery (DaWaK '08), September 1-5, 2008, Turin, Italy.
- The Second International Workshop on Privacy-Aware Location-based Mobile Services (PALMS), April 27, 2008, Beijing, China.
- The Eleventh IEEE International Conference on Computational Science and Engineering, July 16-18, 2008, Sao Paolo, Brazil.
- The Twenty-Second Annual IFIP WG 11.3 Working Conference on Data and Applications Security, July 13-16, 2008, London, UK.
- The First Workshop on Data Mining of Uncertain Data (DUNE 2007), October 28, 2007, Omaha, NE, USA.
- The First Ph.D. Workshop in CIKM (PIKM), November 5, 2007, Lisboa, Portugal.
- The Third International Conference on Information Systems Security (ICISS 2007), December 16-20, 2007, Delhi, India.
- The Third International Workshop on Data Mining and Knowledge Discovery (ADMKD 2007), October 2, 2007, Varna, Bulgaria.
- The Ninth International Conference on Data Warehousing and Knowledge Discovery (DaWaK '07), September 3-7, 2007, Regensburg, Germany.
- The Twenty-Second National Conference on Artificial Intelligence, July 22-26, 2007, Vancouver, British Columbia, Canada.
- Second International Conference on Information Systems Security, December 17-21, 2006, Kolkata, India.
- International Workshop on Privacy Aspects of Data Mining (PADM'06).
- 2006 IEEE International Conference on Data Mining, December 18-22, 2006, Hong Kong, China.
- 2nd ADBIS Workshop on Data Mining and Knowledge Discovery, September 6, 2006, Thessaloniki, Greece.
- 8th International Conference on Data Warehousing and Knowledge Discovery (DaWaK '06), September 4-8, 2006, Krakow, Poland.
- IEEE International Conference on Granular Computing, May 10-12, 2006, Atlanta, Georgia, USA.
- 2005 ACM Symposium on Applied Computing Special Track on Data Mining (DM), March 13-17, 2005, Santa Fe, New Mexico.
- Workshop on Privacy and Security Aspects of Data Mining associated with the Fourth IEEE International Conference on Data Mining, November 1-4, 2004, Brighton, UK.

Proposal Review Panel

- National Science Foundation, April 2008.
- Kentucky Science & Engineering Foundation, November 2006.
- NASA Intelligent Systems Project, January 2004.

Reviewer (only journals listed)

- ACM Transactions on Knowledge Discovery from Data.
- Knowledge and Information Systems, Springer-Verlag, London.
- Journal of Artificial Intelligence Research.
- IEEE Transactions of Knowledge and Data Engineering.

- IEEE Transactions on Systems, Man, and Cybernetics.
- IEEE Transactions on Dependable and Secure Computing.
- Journal of Database Management, Idea Group Inc.
- Journal of Official Statistics, Statistics Sweden.
- Journal of Computer Security, IOS Press, The Netherlands.
- International Journal on Digital Libraries, Springer-Verlag.
- International Journal on Very Large Data Bases, Springer-Verlag.
- Data and Knowledge Engineering, Elsevier.
- Data Mining and Knowledge Discovery, Springer.
- International Journal of Information and Computer Security, Inderscience.

University Service

1. Member, Teaching Methods Innovations Committee, 2005 – 2006
2. Member, Undergraduate - NB Curriculum Committe, 2005 – 2006
3. Member, Undergraduate - NWK Curriculum Committe, 2005 – 2006