Final Report for Period: 09/2010 - 08/2011	**Submitted on:** 09/16/2011
Principal Investigator: Blough, Douglas M.	**Award ID:** 0716252

Organization: Georgia Tech Research Corp

Submitted By:

Blough, Douglas - Principal Investigator

Title:

CT-T: MedVault - Ensuring Security and Privacy for Electronic Medical Records

Project Participants

Senior Personnel

Name: Blough, Douglas
Worked for more than 160 Hours: Yes
Contribution to Project:

Name: Ahamad, Mustaque
Worked for more than 160 Hours: Yes
Contribution to Project:

Name: Sainfort, Francois
Worked for more than 160 Hours: No
Contribution to Project:

Name: Liu, Ling
Worked for more than 160 Hours: Yes
Contribution to Project:

Post-doc

Graduate Student

Name: Bauer, David
Worked for more than 160 Hours: Yes
Contribution to Project:

Name: Kannan, Swagath
Worked for more than 160 Hours: Yes
Contribution to Project:

Name: Bamba, Bhuvan
Worked for more than 160 Hours: Yes
Contribution to Project:

Name: Mohan, Apurva
Worked for more than 160 Hours: Yes
Contribution to Project:

Name: Dacosta, Italo
Worked for more than 160 Hours: Yes
Contribution to Project:

Name: Krishnan, Ramkumar
Worked for more than 160 Hours: Yes
Contribution to Project:

Name: Mashima, Daisuke
Worked for more than 160 Hours: Yes
Contribution to Project:

Name: Palanisamy, Balaji
Worked for more than 160 Hours: Yes
Contribution to Project:

Name: Kulkarni, Aditi
Worked for more than 160 Hours: Yes
Contribution to Project:

Name: Kalgaonkar, Ketan
Worked for more than 160 Hours: Yes
Contribution to Project:

Name: Brown, Jordan
Worked for more than 160 Hours: Yes
Contribution to Project:

Undergraduate Student

Technician, Programmer

Other Participant

Research Experience for Undergraduates

Organizational Partners

Children's Healthcare of Atlanta, Inc.

Other Collaborators or Contacts

We have collaborated with Purdue University (Federica Paci and Elisa Bertino) and Penn State University (Anna Squicciarini) on preserving privacy during trust negotiations. We have also collaborated with Emory University's Center for Clinical Informatics (Saltz, Kurc, and Post) on dynamic access management for biomedical research data sharing environments.

Activities and Findings

Research and Education Activities:
See attached file.

Findings:

See attached file.

Training and Development:

Seven PhD students and 4 MS students have been trained in research methods for information security and privacy, gotten experience with various health information technologies, and been exposed to security/privacy issues for health data.

Outreach Activities:

We have demonstrated various aspects of our project at a number of events sponsored by the Georgia Tech Information Security Center (GTISC) in which the outside community is invited to learn about research being undertaken and technologies being developed at Georgia Tech.

Journal Publications

F. Paci, D. Bauer, E. Bertino, D. Blough, A. Squicciarini, and A. Gupta, "Minimal Credential Disclosure in Trust Negotiations", Identity in the Information Society, p. 221, vol. 2, (2009). Published,

D. Bauer, D. Blough, and A. Mohan, "Redactable Signatures on Data with Dependencies and their Application to Personal Health Records", Proceedings of the ACM CCS Workshop on Privacy in the Electronic Society, p. 91, vol. , (2009). Published,

D. Mashima and M. Ahamad, "Using Identity Credential Usage Logs to Detect Anomalous Service Accesses", Proceedings of the ACM CCS Workshop on Digital Identity Management, p. , vol. , (2009). Published,

D. Mashima, A. Srivastava, J. Giffin, and M. Ahamad, "Protecting E-healthcare Client Devices against Malware and Physical Theft", Proceedings of the 1st Usenix Security Workshop on Health Security and Privacy, p. , vol. , (2010). Published,

A. Mohan and D. Blough, "An Attribute-based Authorization Policy Framework with Dynamic Conflict Resolution", Proceedings of the 9th Symposium on Identity and Trust on the Internet, p. 37, vol. , (2010). Published,

T. Wang and L. Liu, "Output Privacy in Data Mining", ACM Transactions on Database Systems, p. , vol. 36, (2011). Published,

D. Bauer, D. Blough, and D. Cash, "Minimal Information Disclosure with Efficiently Verifiable Credentials", Proceedings of the ACM CCS Workshop on Digital Identity Management, p. 15, vol. , (2008). Published,

F. Paci, D. Bauer, E. Bertino, D. Blough, and A. Squicciarini, "Minimal Credential Disclosure in Trust Negotiations", Proceedings of the ACM CCS Workshop on Digital Identity Management, p. 89, vol. , (2008). Published,

A. Singh, L. Liu, and M. Ahamad, "Privacy Analysis and Enhancements for Data Sharing in *nix Systems", International Journal of Information and Computer Security, p. 376, vol. 2, (2008). Published,

B. Bamba, L. Liu, P. Pesti, and T. Wang, "Supporting Anonymous Location Queries in Mobile Environments with PrivacyGrid", Proceedings of the 17th International World Wide Web Conference, p. , vol. , (2008). Published,

A. Mohan, D. Blough, T. Kurc, A. Post, J. Saltz, "Detection of Conflicts and Inconsistencies in Taxonomy-based Authorization Policies", IEEE International Conference on Bioinformatics and Biomedicine, p. , vol. , (2011). Accepted,

D. Mashima and M. Ahamad, "Enhancing Accountability of Electronic Health Record Usage via Patient-centric Monitoring", Proceedings of the ACM International Health Informatics Symposium, p. , vol. , (2012). Accepted,

R. Zhang, L. Liu, J. Li, and Z. Han, "RBTBAC: Secure Access and Management of EHR Data", Proceedings of the Third International Workshop on e-Healthcare Information Security, p. , vol. , (2011). Published,

R. Zhang and L. Liu, "Security Models and Requirements for Healthcare Application Clouds", Proceedings of the 3rd IEEE International Conference on Cloud Computing, p. , vol. , (2011). Published,

Books or Other One-time Publications

T. Wang and L. Liu, "From Data Privacy to Location Privacy", (2008). Book, Published
Editor(s): J. Tsai and P. Yu
Collection: Machine Learning in Cyber Trust: Reliability, Security, Privacy
Bibliography: Springer-Verlag

D. Mashima, M. Ahamad, D. Bauer, and D. Blough,, "User-centric Identity Management Architecture using Credential-holding Identity Agents", (2011). Book, Accepted
Editor(s): S. Das-Smith, M. Gupta, and R. Sharman
Collection: Digital Identity and Access Management: Technologies and Frameworks
Bibliography: IGI Global

Web/Internet Site

URL(s):
http://medvault.gtisc.gatech.edu
Description:
Project Web site

Other Specific Products

Contributions

Contributions within Discipline:
See attached file.

Contributions to Other Disciplines:

Contributions to Human Resource Development:
See attached file.
Contributions to Resources for Research and Education:

Contributions Beyond Science and Engineering:
See attached file.

Conference Proceedings

Mohan, A;Blough, DM, AttributeTrust - a Framework for Evaluating Trust in Aggregated Attributes via a Reputation System, "OCT 01-03, 2008", SIXTH ANNUAL CONFERENCE ON PRIVACY, SECURITY AND TRUST, PROCEEDINGS, : 201-212 2008

Parameswaran, R;Blough, DM, Privacy preserving collaborative filtering using data obfuscation, "NOV 02-04, 2007", GRC: 2007 IEEE INTERNATIONAL CONFERENCE ON GRANULAR COMPUTING, PROCEEDINGS, : 380-386 2007

Mashima, D;Ahamad, M;Kannan, S, User-Centric Handling of Identity Agent Compromise, "SEP 21-23, 2009", COMPUTER SECURITY - ESORICS 2009, PROCEEDINGS, 5789: 19-36 2009

Wang, T;Meng, SC;Bamba, B;Liu, L;Pu, C, A General Proximity Privacy Principle, "MAR 29-APR 02, 2009", ICDE: 2009 IEEE 25TH INTERNATIONAL CONFERENCE ON DATA ENGINEERING, VOLS 1-3, : 1279-1282 2009

Wang, T;Liu, L, Butterfly: Protecting output privacy in stream mining, "APR 07-12, 2008", 2008 IEEE 24TH INTERNATIONAL CONFERENCE ON DATA ENGINEERING, VOLS 1-3, : 1170-1179 2008

Singh, A;Liu, L, SHAROES: A data sharing platform for outsourced enterprise storage environments, "APR 07-12, 2008", 2008 IEEE 24TH INTERNATIONAL CONFERENCE ON DATA ENGINEERING, VOLS 1-3, : 993-1002 2008

Wang, T;Liu, L, XColor: Protecting General Proximity Privacy, "MAR 01-06, 2010", 26TH INTERNATIONAL CONFERENCE ON DATA ENGINEERING ICDE 2010, : 960-963 2010

Categories for which nothing is reported:

Any Product

Contributions: To Any Other Disciplines

Contributions: To Any Resources for Research and Education

Final Report – CNS-CT-0716252

MedVault: Ensuring Security and Privacy for Electronic Medical Records

Douglas M. Blough, Mustaque Ahamad, and *Ling Liu*
School of Electrical and Computer Engineering
School of Computer Science
Georgia Institute of Technology

Executive Summary

The overall goal of this project was to develop new techniques for the storage, maintenance, and control of sensitive data that permit open sharing among a wide variety of legitimate users while protecting the data against unauthorized use and disclosure. As part of the project, we conducted fundamental disciplinary research in information security and privacy, and also carried out applied research on security techniques for health information systems. Our research resulted in 24 refereed publications, which appeared or are scheduled to appear as 2 book chapters, 4 journal papers, and 18 refereed conference publications. We believe our research has strong potential to impact the future of health information systems by allowing patients to control the access and use of their health information, while still providing the benefits of electronic records and information sharing to the health system. These benefits include improving quality and safety of patient care and allowing aggregation of electronic health record data for medical research purposes.

In addition to Georgia Tech's partnership with Children's Healthcare of Atlanta, this project led to several new collaborations between our privacy and security researchers and medical organizations. First, we have been collaborating for the past year with Emory University's Center for Clinical Informatics (CCI) on attribute-based security for biomedical research data sharing systems. In addition to being partially funded through this grant, seed funding for this collaboration was provided by the Atlanta Clinical and Translational Sciences Institute (ACTSI), which is funded by the NIH CTSA program. Although in its very early stages, this research collaboration has already produced a joint publication between MedVault researchers and Emory CCI [13]. We have also begun discussions with the Georgia Cancer Coalition (GCC) on how to provide patients more control over their health data within a state-wide health information exchange (HIE). In the future, we plan to apply our initial research on patient-centric approaches to health information management to a GCC project, funded by the Department of Health and Human Services, on how to involve patients more actively in their medical care.

Research Activities and Findings

The major activities we carried out in this project fall into two categories: fundamental disciplinary research in security and privacy for identity and access management, and application of our approaches to health information sharing. Our disciplinary research had two major thrusts: identity and access management in information sharing environments, and data/location privacy. Next, we discuss our research in these two thrusts, as well as the application of our work in healthcare scenarios.

Identity and Access Management

Our identity and access management research has been carried out in the context of attribute-based systems. In attribute-based systems, identity is established and authorizations are granted based on attributes of the participating entities, rather than solely on user names and passwords. To enable attribute-based systems, it is necessary to have methods for certifying and verifying attributes. Our research has invented novel approaches to digital credentials [2, 14, 15] for supplying verifiable attributes and also a reputation-based system for evaluating trust in attributes [11]. We developed and prototyped the concept of an identity agent [6, 7], which holds attributes for a user and releases them according to the user's policies or via direct authorization. Policies are an important part of attribute-based systems. Our work also proposed new methods for performing dynamic conflict resolution among multiple policies [12] and for carrying out dynamic conflict and inconsistency detection among hierarchical policies [13]. Finally, careful monitoring is required to ensure that sensitive personal information does not fall into the wrong hands. We have proposed and evaluated several techniques for monitoring operations involving credentials and other sensitive personal information such as health data [4, 5]. Next, we briefly discuss some of our contributions on these topics.

Our research developed a new type of digital credential, which we refer to as a "minimum disclosure digital credential" [2]. This credential uses redactable signature technology, which allows a certificate authority to create and sign a credential containing many different user attributes. Through a redaction operation, the user can then disclose only the attributes required to authorize a particular operation, while still permitting the relying party to verify those attributes based on the certificate authority's signature on the entire credential. In addition to presenting a scheme for applying redactable signatures in the context of digital credentials, this work also extended the redactable signature concept to multiple authorities, thereby allowing a single credential to hold attributes signed by different authorities. In related work, we showed how this minimum disclosure credential could be used within an overall framework for trust negotiation between different parties [14, 15].

We also applied redactable signatures to the problem of selectively disclosing health information [3], while still being able to verify cryptographically the source of the information. This allows the source of health information to be traced even as it is relayed multiple times between different entities. An example use, given in [3], is for a patient to store an entire signed health record from a medical provider, while then being able to disclose selected parts of the record to other entities and still allow those entities to cryptographically verify the medical provider as the source of the information. In the context of this work, we identified a need for sources of data to limit the ways in which the data can be redacted as it is relayed by other parties. We allow these "redaction policies" to be specified as disclosure dependencies between different data items in the data set. In [3], we show how these dependencies can be encoded into the hash tree structures, which are used in redactable signature techniques. We thus provided the first redactable signature technique with source disclosure policies encoded into the signature.

Our project also pioneered the concept of identity agents, which manage personal information for users. In [6], we proposed an identity management architecture using identity agents, which manage a user's attributes under the user's control, and we showed how this architecture solves security, usability, and privacy issues inherent in existing user-centric identity management systems. We also developed and evaluated a scheme for handling identity agent compromises [7]. In this work, we considered how to allow a user to turn credential monitoring on and off while still providing safe operation when monitoring is off. This approach combines an in-network monitoring agent with group signature technology and a separate device carried by the user, such as a secure USB key. In normal operation, all identity-related operations must be made known to the in-network monitoring agent in order to be authorized. However, if the user wishes to bypass the monitoring agent for certain very sensitive operations, then he/she can do so by providing the separate secure device as a second authentication factor.

When credential use is monitored, e.g. using the approach just described, we would like to develop techniques to detect potential misuse of the credentials. This is the topic of [4], where we describe an anomaly-based metric to generate risk scores for particular credential usages, based on the past history of user activity. In the area of identity and access monitoring, we also considered how to monitor access to electronic health records so as to inform individual patients as to when and how their health information is being accessed [5]. This work is discussed in more detail below.

In [12], we presented and evaluated a framework for dynamic policy composition and conflict resolution in federated environments. In environments such as health information exchanges, there are multiple entities that specify access policies, e.g. the patient, the health care provider, and the information exchange. How to combine these different policies and resolve conflicts that arise among them is an important issue. Our framework eliminates the need to recompose policies if the policy combination algorithm is changed. It provides a novel method to dynamically add and remove specialized policies, while retaining the clarity and modularity in the policies. The proposed framework also provides a mechanism to reduce the set of potential target matches, thereby increasing the efficiency of the evaluation mechanism. Similarly, in large complex data sets, data types are often specified in hiearchies and access policies can be specified at different levels. Our work in [13] considers how to dynamically detect conflicts between policies specified on large complex data sets. One interesting use of our algorithm is to detect vulnerabilities to inference attacks by detecting access policy inconsistencies between highly correlated data items.

Privacy

In our work on privacy-conscious data sharing, we designed and evaluated algorithms for privacy-preserving searches in enterprise storage environments [18], and we identified privacy violations that arise from improper use of access control capabilities in Unix-based environments [19]. We also studied the problems of privacy preserving collaborative filtering, data access, and data mining, identified the problem of output privacy and developed a scalable solution for protecting output privacy, especially in data stream based access and mining [17, 21]. We also developed the PrivacyGrid framework for scaling anonymous location-based data access and queries, which provides one of the essential components for location-dependent access-control-enabled sharing of electronic medical record data [1]. In related work, our research on location privacy [20] can be applied to tracking of patients and other individuals within a hospital-type environment.

We have also defined the novel concept of proximity privacy [22, 24]. In a proximity privacy breach, an attacker learns with high confidence that the sensitive information of a victim is associated with a set of semantically proximate values, even though the exact one is not revealed. This is a concern, for example, with electronic medical records of patients. This paper presents XCOLOR, a novel anonymization model that is targeted at proximity privacy, with theoretical guarantees on both operation efficiency and utility preservation. A second paper considers the problem of output privacy in data mining [23]. Privacy preservation in data mining demands protecting both input and output privacy: the former refers to sanitizing the raw data itself before performing mining; while the latter refers to preventing the mining output (models or patterns) from malicious inference attacks. This work provides a systematic study of the problem of protecting output privacy in data mining from three perspectives. We first analyze the importance of this problem by showing that even sufficient protection of input-privacy does not guarantee that of output-privacy. We then propose a light-weight countermeasure that can effectively eliminate these breaches without explicitly detecting them, while minimizing the loss of the output accuracy. We further optimize the basic scheme by taking account of two types of semantic constraints, aiming at maximally preserving utility-related semantics while maintaining hard privacy guarantee.

Application to Health Information Sharing

Much of our research described above has been applied to, and evaluated in, the context of health information systems. For example, our redactable signature work was applied to the dissemination of electronic health records via a personal health record (PHR) service [3]. We have developed a prototype for a PHR service that uses our redactable signature scheme as a core component. This prototype permits patients to selectively disclose information from their PHRs to third parties while preserving integrity and source verifiability of the data. In [3], we describe the operation of this source-verifiable PHR service with selective disclosure and evaluate its performance. This paper also describes how to extend our basic redactable signature scheme to deal with disclosure dependencies between different parts of the medical record. We have also developed a prototype demonstration system that provides emergency responder access to health information via our prototype PHR service, and we have written a technical report describing the operation of this overall system [10].

Our work on monitoring has been applied in the context of electronic health record access [5]. In this work, we introduce the notion of accountable use and update of electronic health records and design a patient-centric monitoring system based on it. We develop a system architecture and associated protocols that enable either explicit or implicit patient control over when and how health information is accessed. Our approach provides a reasonable solution rather than addressing the more general distributed information flow control problem, which can not be solved without making assumptions that are unlikely to hold in widely deployed health information sharing systems. We also implement and evaluate a prototype system motivated by a health record sharing scenario based on NHIN Direct to demonstrate that enhanced accountability can be supported with acceptable performance and integration overheads.

Our work on detection of conflicts and inconsistencies among hierarchical policies has been evaluated in the context of medical data [13]. Policies were defined across the i2b2 medical ontology, which provides a comprehensive classification of medical data types. Conflict detection algorithms were then proposed and evaluated using the i2b2 ontology. We also demonstrated the potential of our algorithms to detect inference attack vulnerabilities by detecting access policy inconsistencies between different but highly correlated data elements. For example, a policy might say that a patient's HIV status can only be disclosed to a very limited set of users. However, other data elements in a medical record might be highly correlated with HIV status, e.g. the use of antiretroviral drugs. Our algorithms can detect that the policy covering access to data on this type of medication is more lenient than the policy covering access to HIV status and it will raise warnings that a policy adminstrator can use to properly align the policies.

In other work, we have begun investigating the security issues and potential solutions in storing health records in the cloud [25, 26] and we proposed an architecture that can protect client devices of e-healthcare systems (e.g., laptop PCs and smartphones) from malware-based attacks as well as physical theft [8].

Contributions

Contributions within Discipline

We have made multiple novel contributions to the areas of identity and access management and data/location privacy. These include:

- the concept of an identity agent, which stores, manages, and selectively discloses sensitive personal information on behalf of users,
- architectures, algorithms, and credential types to support identity agents,
- algorithms for detection of identity agent compromise and identity credential misuse,
- an architecture and protocols for accountable use of electronic health information,
- a framework for permitting efficient dynamic policy composition in complex policy-driven information sharing environments,
- algorithms for detecting policy conflicts and inconsistencies among hierarchical policies,
- redactable signature schemes that work with disclosure dependencies among data items,
- the concept of proximity privacy and novel anonymization techniques for achieving it, and
- algorithms for achieving location privacy while maintaining utility of location-dependent services.

More information about these contributions are provided earlier in this report and complete details are contained in the papers referenced at the end of this report.

Contributions beyond Science and Engineering

Our work targets secure and privacy-conscious health information sharing, which fills a critical societal need. We are specifically targeting two health care use case scenarios: "Consumer Access to Clinical Information" and "Emergency Responder Access to Electronic Health Information". We have developed a prototype demonstration system targeting the emergency responder scenario and making use of some of the technologies developed in the project. A video of this prototype demonstration is available on the MedVault project Web site [9]. We have also collaborated with Emory University's Center for Clinical Informatics (CCI), where we are investigating how our security and privacy approaches can be used within a health information exchange that CCI is developing for biomedical research use. Our work on attribute-based authorization policies, dynamic policy combination, and detection of policy conflicts and inconsistencies is currently being integrated into the CCI research data exchange software.

Contributions to Education and Human Resources

During the period of this grant, seven PhD students, Bhuvan Bamba, David Bauer, Jordan Brown, Italo Dacosta, Daisuke Mashima, Apurva Mohan, and Balaji Palanisamy, and four M.S. students, Ketan Kalgaonkar, Swagath Kannan, Ramkumar Krishnan, and Aditi Kulkarni, worked part-time or full-time on this project. David Bauer, Bhuvan Bamba, and Apurva Mohan all completed their Ph.D. degrees with the support of this award. Dr. Bauer's dissertation research involved privacy-preserving and user-centric approaches to identity and access management. His research contributed to six publications associated with this project [2, 3, 6, 10, 14, 15]. He is now employed at Army Research Laboratories. Dr. Bamba's dissertation work was on location privacy and contributed to three of the project's publications [1, 10, 24]. He is currently working for Oracle. Dr. Mohan worked on dynamic policy analysis. His dissertation research contributed to five project publications [3, 10, 11, 12, 13]. He is currently in a research group at Honeywell. Mr. Mashima is nearing the end of the PhD program and has been working on identity and access monitoring. To date, his dissertation research has contributed to six publications associated with the project [4, 5, 6, 7, 8, 10]. The other PhD students have recently entered the PhD program.

Results from the research have been incorporated into the graduate-level course on "Secure and Dependable Distributed Systems", taught by PI Blough. One new course module on Federated Identity and Access Management was included in the Spring 2009 course offering and a second on Secure and Privacy-Conscious Sharing of Medical Data was added in the Fall 2010 offering.

References

[1] Bhuvan Bamba, Ling Liu, Peter Pesti and Ting Wang, "Supporting Anonymous Location Queries in Mobile Environments with PrivacyGrid," *Proceedings of 17th International World Wide Web Conference,* 2008.

[2] D. Bauer, D. Blough, and D. Cash, "Minimum Information Disclosure with Efficiently Verifiable Credentials," *Proceedings of the 4th Workshop on Digital Identity Management,* pp. 15–24, 2008.

[3] D. Bauer, D. Blough, and A. Mohan, "Redactable Signatures on Data with Dependencies and their Application to Personal Health Records," *Proceedings of the ACM CCS Workshop on Privacy in the Electronic Society* (WPES), pp. 91–100, Nov. 2009.

[4] D. Mashima and M. Ahamad, "Using Identity Credential Usage Logs to Detect Anomalous Service Accesses," *Proceedings of the 5th ACM CCS Workshop on Digital Identity Management,* Nov. 2009.

[5] D. Mashima and M. Ahamad, "Enhancing Accountability of Electronic Health Record Usage via Patient-centric Monitoring," *Proceedings of the ACM International Health Informatics Symposium,* 2012, to appear.

[6] D. Mashima, M. Ahamad, D. Bauer, and D. Blough, "User-centric Identity Management Architecture using Credential-holding Identity Agents," in *Digital Identity and Access Management: Technologies and Frameworks,* ed. S. Das-Smith, M. Gupta, and R. Sharman, to appear.

[7] D. Mashima, M. Ahamad, and S. Kannan, "User-Centric Handling of Identity Agent Compromise," *Proceedings of the 14th European Symposium on Research in Computer Security* (ESORICS), Sept. 2009.

[8] D. Mashima, A. Srivastava, J. Giffin, and M. Ahamad, "Protecting E-healthcare Client Devices against Malware and Physical Theft," *Proc. of 1st USENIX Workshop on Health Security and Privacy* (HealthSec), Aug. 2010.

[9] MedVault project Web site, http://medvault.gtisc.gatech.edu.

[10] A. Mohan, D. Bauer, D. Blough, M. Ahamad, B. Bamba, R. Krishnan, L. Liu, D. Mashima, and B. Palanisamy, "A Patient-centric, Attribute-based, Source-verifiable Framework for Health Record Sharing," GIT CERCS Technical Report No GIT-CERCS-09-11, 2009. (available at http://medvault.gtisc.gatech.edu/)

[11] A. Mohan and D. Blough, "AttributeTrust: A Framework for Evaluating Trust in Aggregated Attributes via a Reputation System," *Proceedings of the Annual Conference on Privacy, Security, and Trust,* pp. 201–212, 2008.

[12] A. Mohan and D. Blough, "An Attribute-based Authorization Policy Framework with Dynamic Conflict Resolution," *Proceedings of the 9th Symposium on Identity and Trust on the Internet* (IDTRUST), pp. 37–50, 2010.

[13] A. Mohan, D. Blough, T. Kurc, A. Post, and J. Saltz, "Detection of Conflicts and Inconsistencies in Taxonomy-based Authorization Policies," *Proceedings of the 2011 IEEE International Conference on Bioinformatics and Biomedicine,* to appear.

[14] F. Paci, D. Bauer, E. Bertino, D. Blough, and A. Squicciarini, "Minimal Credential Disclosure in Trust Negotiations," *Proceedings of the 4th Workshop on Digital Identity Management,* pp. 89–96, 2008.

[15] F. Paci, D. Bauer, E. Bertino, D. Blough, A. Squicciarini, and A. Gupta, "Minimal Credential Disclosure in Trust Negotiations," *Identity in the Information Society,* Oct. 2009.

[16] R. Parameswaran and D. Blough, "Privacy Preserving Collaborative Filtering using Data Obfuscation," *Proceedings of the IEEE International Conference on Granular Computing,* pp. 380–386, 2007.

[17] R. Parameswaran and D. Blough, "Privacy Preserving Data Obfuscation for Inherently Clustered Data," *International Journal of Information and Computer Security,* Vol. 1, pp. 4–26, 2008.

[18] A. Singh and L. Liu, "SHAROES: A Data Sharing Platform for Outsourced Enterprise Storage Environments," *Proceedings of the IEEE International Conference on Data Engineering,* 2008.

[19] A. Singh, L. Liu, and M. Ahamad. "Privacy Analysis and Enhancements for Data Sharing in *nix Systems," *International Journal of Information and Computer Security,* Vol. 2, pp. 376–410, 2008.

[20] T. Wang and L. Liu, "From Data Privacy to Location Privacy," in *Machine Learning in Cyber Trust: Reliability, Security, Privacy,* edited by J. Tsai and P. Yu, Springer-Verlag, 2008.

[21] T. Wang and L. Liu, "Butterfly: Protecting Output Privacy in Stream Mining," *Proceedings of the IEEE International Conference on Data Engineering,* 2008.

[22] T. Wang and L. Liu, "XColor: Protecting General Proximity Privacy", *Proc. of 26th IEEE International Conference on Data Engineering,* pp. 960–963, 2010.

[23] T. Wang and L. Liu, "Output Privacy in Data Mining", *ACM Transactions on Database Systems,* vol. 36, March 2011.

[24] T. Wang, S. Meng, B. Bamba, and L. Liu, "A General Proximity Privacy Principle," *Proceedings of the 25th IEEE International Conference on Data Engineering,* pp. 1279–1282, 2009.

[25] R. Zhang and L. Liu, "Security Models and Requirements for Healthcare Application Clouds," *Proceedings of the 3rd IEEE International Conference on Cloud Computing,* 2011.

[26] R. Zhang L. Liu, J. Li, and Z. Han,"RBTBAC: Secure Access and Management of EHR Data," *Proceedings of the 3rd International Workshop on e-Healthcare Information Security,* 2011.