Three Pillars of Trust: Privacy, Identity Management and Compliance[1]

B. Ramamurthy
CSE Department
University at Buffalo, SUNY
Amherst, NY 14260
716-645-3180 (108)
bina@cse.buffalo.edu

S. Abhyankar
CSE Department
University at Buffalo, SUNY
Amherst, NY 14260-2000
surabhia@cse.buffalo.edu

Abstract

In this paper we present details of a critical requirement of many systems, namely, trust. Trust is one of the oldest issues that has taken a new incarnation with advent of the Internet. In the context of the Internet and the scientific and commercial applications it has enabled, definition of trust stands to be rewritten and reviewed. Our research indicates that privacy, identity management, and compliance form the three pillars of trust. Privacy is extremely important to people, and governments have enacted laws to guard privacy. Organizations are working towards complying with privacy regulations. Identity management has been leveraged to provide the compliance. In this paper we present general concepts related to privacy, identity management and compliance to regulations. We will provide a comprehensive coverage of identity management concepts. Identity management cannot be discussed without privacy and compliance context. We introduce privacy and compliance concepts along with some representative laws. Stakeholders of identity management and related concepts span almost the entire spectrum of information technology users from hospitals, research labs, universities, government agencies to commercial business including financial institutions.

1. Introduction

Most application areas nowadays deal with rich collections of data and sophisticated data-intensive software applications. Large amounts of data are collected and shared among researchers in such areas as high performance computation (HPC) [11] and bioinformatics [2]. Hospitals by the nature of their business collect information about patients and the data collected is made available for researchers. Businesses collect large amounts of user information that are analyzed by statisticians and data mined for user management purposes. A fundamental requirement for all these processes is that data is not compromised either deliberately or inadvertently. In many cases data is associated with identity of a person; it is important that privacy, confidentiality and integrity of personal identity are guaranteed when the non-identifying data is used for research or business purposes. Owner of the identity should be aware of its use and must have a choice to opt out of the process. It is imperative that digital identity of people is preserved and protected by auditable processes. Governments across the globe have recognized the importance of this and have enacted several laws to govern identity related data. Organizations are working diligently on complying with these laws. Related operations affect e-commerce and computing at all levels including data collection and computing areas. Main motivation of this paper is to spread awareness of these fundamental concepts to improve the technical preparedness of workforce in the areas for the emerging concepts: privacy, identity management and compliance to regulations.

[1] Partial support for this work was provided by the National Science Foundation's Course, Curriculum, and Laboratory Improvement program under grant DUE-0311473

We discuss background information on the concepts in Section 2, details of components of identity management in Section 3, and significant contributions of the work are summarized in Section 4.

2. Background

We discuss here the current state of identity management, privacy management, and compliance with legislations such as Privacy Act of 1974 [4], HIPAA (Health Insurance Portability and Accountability Act) and FERPA (Family Educational Rights and Privacy Act). Although there are many other interesting topics related to identity management such as security we are limiting the scope to the three main issues in order to provide a comprehensive coverage of the focus area.

2.1 Identity and Identity Management

Identity is information about an entity. When we represent the physical identity using a digital format we get what is known as digital identity [3]. We will use "identity" to refer to "digital identity". Though it is usually associated with a human being, identity is also associated with systems, applications, services and devices that act on behalf of a person. It also can be associated with non-human entities such as a pet dog and inanimate objects such as nuclear war-head, truck carrying food or a building. We will limit the scope of this paper to identity of human subjects. Moreover humans offer a very interesting identity challenges that are unique such as variety and dynamic nature of identity information. A person's identity information can be used for different purposes. Person's visa card number can be used as an identifier, mother's maiden name as authenticator, and personal identification number (PIN) as authorizer for withdrawing money. Identities are the core of any organization [6, 7] and must be protected from misuse.

Identity management involves processes and policies related to the creation, use and termination of digital identity. It enables efficient, safe and secure access to data, systems and applications [7]. Identity management is essential for security of a system, to establish trust in a system, for user management, for monitoring illegal and criminal activities, for establishing compliance with the law, to support auditing and reporting process, for provisioning, for access control and protection of resources and maintaining confidentiality and protection of information. Spatial and temporal limitations of an identity are managed by identity management methods. For example, when a student joins a research team she is provided resources ("provisioning concept") and privileges based on her identity and these are reclaimed or annulled when she leaves the team. We have discussed in Section 3 a comprehensive set of relevant concepts that define identity management.

2.2 Privacy and Privacy Management

Privacy is the ability an individual has in controlling the handling of data about him or herself [4, 6]. Privacy has always been in the fore front of our constitution with several amendments protecting individuals [23]. Concern about electronic records became hot topic for congressional debates in the 1960's with the advent of commercial computers. Since then many laws have been enacted by the U.S. government and we will limit our discussion to two representative regulations. We will introduce the Privacy Act of 1974 and discuss technical details of HIPAA and FERPA regulations. Privacy management involves establishing policies and implementing processes to comply with privacy rules.

2.3 Privacy Act 1974

Privacy Act of 1974 prohibits any federal systems from releasing electronic records pertaining to a person without written consent from the person to whom the records pertain. Privacy has been further specialized for data records collected in a health care domain and for data pertaining to students in educational environments. Several other rules exist for other domains such as financial, auditing and homeland security and so on.

2.4 HIPAA Privacy Rule

Each time a patient sees a doctor, is admitted to a hospital, goes to a pharmacist or sends a claim to a health plan, a record is made of their confidential

health information. In the past, family doctors and other health care providers protected the confidentiality of those records by sealing them away in file cabinets and refusing to reveal them to anyone else. Today, the use and disclosure of this information is protected by a patchwork of state laws, leaving gaps in the protection of patients' privacy and confidentiality. The Health Insurance Portability and Accountability Act of 1996 (HIPAA), was the result of efforts by the Clinton Administration and congressional healthcare reform proponents to reform healthcare. The goals and objectives of this legislation are to streamline industry inefficiencies, reduce paperwork, and make it easier to detect and prosecute fraud and abuse and enable workers of all professions to change jobs, even if they (or family members) had pre-existing medical conditions. In this paper we will limit the scope to data record management and identity management aspects of the regulation. Accordingly the following are aspects of HIPAA are relevant to a scientist: (i) information about patients is protected, (ii) consumers have control over their information, (iii) provide education to patients and proper access to their own records, (iv) strict boundaries on medical records use and release, (v) releasing minimum amount of information as necessary, (vi) ensure security of personal information and (vii) establish accountability for all use and releases.

2.5 FERPA Rule

Family Educational Rights and Privacy Act (FERPA) [47] protects privacy of student education records. The law applies to all schools that receive funds from U.S. Department of Education. It gives parents and students over 18 certain rights over student's records. It prevents schools from releasing certain information without written consent from an eligible student or a parent. Transfer of student records for the normal operation of the schools such as grading, assessment, auditing, and accreditation are permitted without consent from the student or parent.

2.6 Compliance to Regulations

Compliance is about the integrity of the systems that support organizations in their efforts to comply to regulations such as Privacy Act, FERPA and HIPPA. We are moving into a culture of compliance to establish trust and assure integrity for paperless electronic record keeping. Most universities have established boards and committees to evaluate their compliance readiness to regulations and have established an auditable set of policies and their implementation methods. In spite of establishment of offices for compliance, actual compliance methods are still arcane with electronic records spread around many data bases typical in an organization. Compliance involves (i) establishing policies, (ii) devising strategies to implement policies, (iii) implementing strategies and processes to enforce policies, and (iv) establishing auditing processes to assure compliance. Since core of these regulatory measures pertain to electronic records and privacy of identities, identity management has emerged as compelling solution [42] for complying with regulations. As an example, consider the importance of de-identification when releasing medical records explained in Section 3. Compliance requirements have created an employment market for people knowledgeable about scientific methods as well as regulatory methods.

3. Identity Management

Current subtopic selection in Figure 1 is based on informal interviews with stakeholder and domain experts and on existing literature. As shown on the identity list of Figure 1, there are different types of identity information. Date of birth and place are static while work address may be changing. Color of skin is strong identity whereas dress color is weak identity (Ex: woman in pink coat) that may expire after a period of time. There is a whole dictionary of terms used to describe identity that ontology management has become an interesting area of research [45]. De-identification is removal of privacy revealing information from data while re-identification is constructing an identity using information from various sources. The subtopic of *Models for identity management* is another interesting problem and many prominent industries are involved in this. Microsoft has an application called Passport [17] that can aggregate identities of its users and serve these to authorized third parties. A catch here is that Microsoft's model is a virtual central repository model under Microsoft's control. Many

other companies have formed a consortium called Liberty Alliance Project [15] that proposes a federated and open standard for identity management system. We will discuss in detail topics listed in Figure 1.

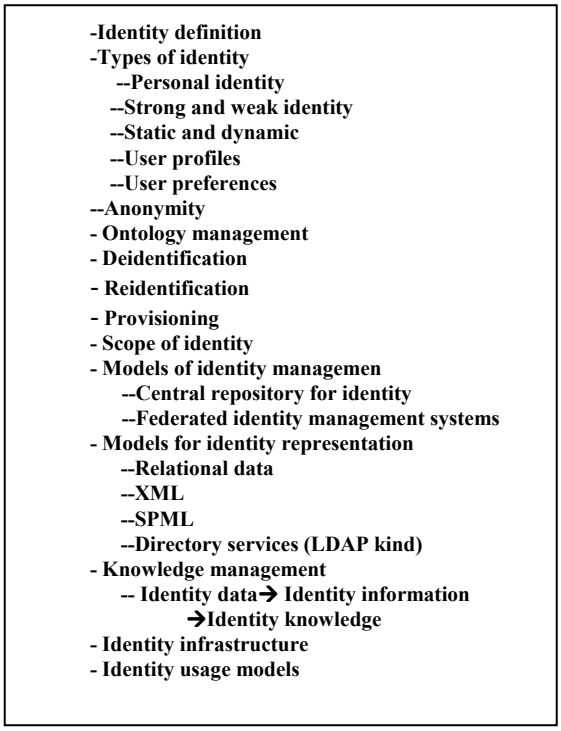

Figure 1 Identity Management Concepts

3.1 Definition

Identity management is the set of processes, tools, and social contracts surrounding the creation, maintenance, utilization and termination of a digital identity for people, systems and services to enable secure access to an expanding set of systems and applications.

3.2 Types of Identity

Personal Identity: Personal information about a user constitutes the personal identity. This includes name, age, current address, SSN, height, weight and the like.

Static and dynamic identity: Static identity is something that is permanent about an entity and it never changes. It includes details such as SSN, eye color, hair color, birthmarks etc. Dynamic identity can include features that may change. For example, weight.

User profiles: Details about a user are maintained to customize an environment or experience to meet the needs of a user. In this case, typically the user gives out information willingly. For example, a frequent business traveler specifying the room type to be selected automatically every time he/she makes a reservation.

User preferences: Often user details are captured by the products they purchase or actions they take in response to a situation. When you make a purchase using a special shopper's card you are providing data related to your preference of products to market researchers.

3.3 Anonymity

Anonymity is a feature by which the user can choose not to divulge some or any of the details in his identity. It provides the consumer with utmost privacy. However, anonymity has its repercussions. It becomes difficult to trace back to the individual incase of any eventualities. Re-identification is used to deal with such situations.

3.4 Ontology management

One of the major concerns of identity management is storage of identities. While, identities of users may have many factors in common, the possibility of minor differences cannot be ruled out. There is a necessity of a common semantic schema that can be used to create user identities. Also, the administrator should be able to change the schema incase a change in the profile structure is desired.

Ontology is an exhaustive conceptual schema about a domain. It is a hierarchical structure that contains all the entities and their relationships and rules within that domain. Ontologies can be used to build a schema for identity profiles.

3.5 Deidentification

De-identification is the process of removing identifiable parts of data about an entity held at an organization before releasing it to the third party. Thus, the third party cannot trace the entity from the available data. For example when releasing clinical data for data mining research it goes

through an auditable process of deidentification to assure compliance with HIPAA privacy rules. De-identification is carried out in several stages. In each stage, sensitive data is replaced. Data types are defined as "sensitive" depending on the HIPAA compliance policies and the institutional policies. It is possible to infer some information from certain query results. For example, consider a company who wants to open a factory in an isolated village. The factory will do wonders for the economy of the village. The company needs cheap labor. Hence, it collaborates with a third party, for instance, the census bureau that has information about the number of people living there, their age groups etc. The query on the percentage of population in various age groups might give results from which the availability of labor can be inferred. This compromises on the privacy of the villagers. Therefore, such results need to be edited. Natural language processing (NLP) is used to perform pluggable de-identification, i.e, search and replace sensitive data.

3.6 Reidentification

Anonymity is an important means of protecting the privacy of the users. But certain users can abuse this privilege by hacking into the system. But if this feature is removed, the user's ability to protect their privacy is severely restricted. Thus, misuse of system resources is prevented by compromising on privacy. A solution that offers privacy and a means to track miscreants is the use of false names in place of real ones. The process of mapping the used identity to the real identity of the miscreant is called Re-identification. Re-identification also has a potential for misuse. The system operator is responsible for mapping the real user identities to false identities and vice versa. Incase the system operator is in collaboration with the hacker, he can use the translation of names to false names to their advantage. Therefore, for this scheme to work, the system operator must be trustworthy.

3.7 Provisioning

An identity is referred to by its identifier. Upon creation, every identity is associated with an identifier. It is then linked to the authentication providers. During the lifetime of the identity, its attributes and privileges are subject to change. Also, an identity should be destroyed when the need arises. Provisioning in the context of identity management involves creation, linkages, sharing, modification and updating, destruction of identities. Sharing of identities implies transactional transfer of data to affiliated organizations that do not have direct access to the corresponding repository.

3.8 Scope of Identity

We can analyze relevance and validity of identity based on the temporal and spatial scope of its attributes as discussed below.

Temporal Scope: Identities define the individuality about a person. Certain aspects of the user profile may change over time (temporal attributes). Temporal scope of an identity defines the validity of an identity over a period of time. Hence, if the temporal attributes are consistent with time, the identity is valid. Consider the age of a user. Age is a temporal attribute. The profile of the user needs to be updated every year to reflect increase in the age.

Spatial Scope: Spatial scope defines the extent of the identity and its relation to other identities. It can also define the use of a particular identity for a given range of applications. A consumer might have multiple identities. For example, a user may be a doctor by profession, and he may attain an identity of a shopper while buying things. The shopper profile includes his preferences in items and his primary profile lists his professional qualifications. The spatial scope of the shopper identity is used only when the doctor is purchasing items and not when he is dispensing medical advice online.

3.8 Identity Database Models

Owing to the large number of identities, identity storage and authentication is a significant problem. The following three models discuss different approaches to identity storage and authentication.

3.8.1 Single source proprietary model

According to this model, a consumer can use single name and password to logon to all the

participating sites and services. A block diagram of this model is shown in Figure 2.

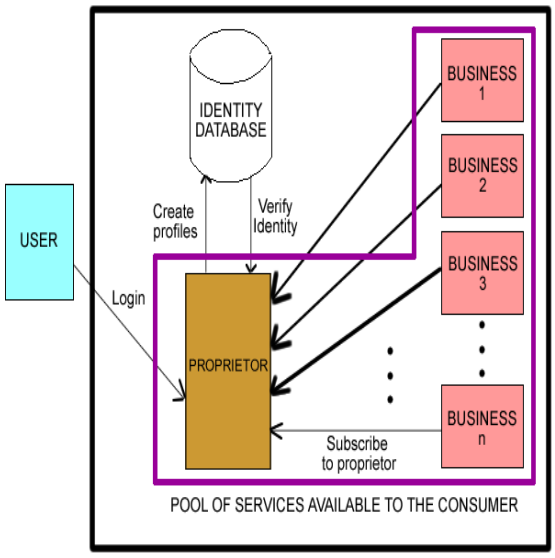

Figure 2 Single Source Proprietary Model

The proprietor of the scheme in Figure 2 is a company. This company is responsible to store the profiles of the consumers. Profiles are the identities of consumers. The consumer can store personal information while creating the profile and then modify it if desired.

Businesses shown in Figure 2 interested in offering their services to consumers via the central authority collaborate with it. Then the managing authority dispenses user information to the affiliated companies. The consumer simply has to agree to the terms and conditions set forth by the central authority. This model necessitates the central authority to authenticate all the users thereby creating a bottleneck. Example for this model is Microsoft's Passport [ref].

3.8.2. Federated Model

The federated model involves creation of an open and interoperable standard for network identity where privacy, security and trust are maintained. In this model shown in Figure 3, the authentication system is decentralized. That is, all the companies maintain an identity database shown as 1, 2, 3..n in Figure 3 of the registered users. The participating businesses form a federation of companies as shown in Figure 3 and create a network of trust across network devices. Thus, the users can sign on from the site of any of the businesses in the federation and then access the services of all the organizations that are a part of that alliance. Hence, the user does not need to register to access the services of allies.

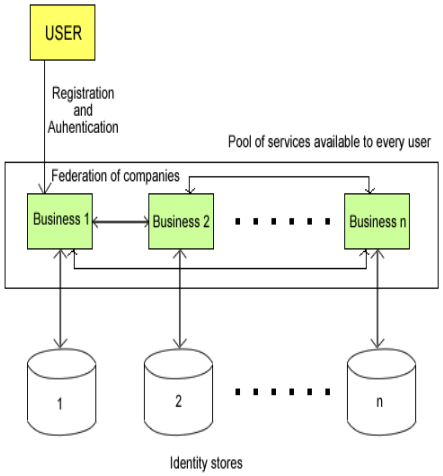

Figure 3 Federated Identity Model

Liberty Alliance [ref] is a consortium of several businesses and it proposes a federated and open standard for identity management system.

3.8.3 Individual Identity Management Model

In this model of identity management, every individual maintains his/her identity on himself/herself. This identity is advertised to the respective organization automatically whenever the user wants to access any services offered by it. Hence, the need for maintaining a database is eliminated.

Social security number is a way of providing a unique identity to every person. But this still requires the user to enter personal information while registering from sites. If a RFID (radio frequency identification) chip that is capable of storing the complete profile of the user, such as, name, age, birth date, distinguishing features etc is inserted into every individual, then the user identity can be floated.

4. Significant Contributions

For example, “1. Introduction”, should be Times 12-point boldface, initially capitalized, flush left, with one blank line before, and one blank line after. Use a period (“.”) after the heading number, not a colon.

Use footnotes sparingly (or not at all) and place them at the bottom of the column on the page on which they are referenced. Use Times 8-point type, single-spaced. To help your readers, avoid using footnotes altogether and include necessary peripheral observations in the text (within parentheses, if you prefer, as in this sentence).

5. References

[1] American Association for the Advancement of Science (AAAS) AAAS/NSF Invention and Impact Conference, Washington DC, April 16-18, 2004. http://www.aaas.org/, last visited May 16, 2005.

[2] B. Bergeron. *Bioinformatics Computing*, Prentice Hall Inc., November 2002.

[3] M. Bishop. *Introduction to Computer Security*, Addison-Wesley Inc., 2005.

[4] A. A. Bushkin and S. I. Schaen. *The Privacy Act of 1974 A Reference Manual for Compliance* published by System Development Corporation (McLean, Virginia), 1975.

[5] E. Chabrow and L. Greenemeier. *Real Id Faces Reality*, Compliance Pipeline, May 16, 2005, http://www.compliancepipeline.com/163102234 , last visited May 16, 2005.

[6] R. Clarke. Dataveillance and Privacy Homepage, Xamax Consultancy Private Ltd., http://www.anu.edu.au/people/Roger.Clarke/DV/ , last visited May 10, 2005.

[7] J.D. Clercq and J. Rouault. *An Introduction to Identity Management*. HP Devloper Resource Central, http://devresource.hp.com/drc/resources/idmgt_intro/index.jsp , last visited 5/4/2005.

[8] A. Cooper and R. Reimann. About *Face 2.0 – The Essentials of Interaction Design*, John-Wiley and Sons, 2003.

[9] The Educational Technology Center at Buffalo (ETC), http://www.etc.buffalo.edu/, last visited May 16, 2005.

[10] D. Eggen. *Carnivore Glitches Botched Bin Laden Probe - FBI Memo*, Newsbytes, 29 May 2002, http://www.mafhoum.com/press3/99T42.htm, last visited May 16, 2005.

[11] I. Foster and C. Kesselman, editors. *The Grid 2: Blueprint for a New Computing Infrastructure*. Morgan Kaufmann, 2004.

[12] P. Gopalam, B. Ramamurthy and A. Cartwright. *Java Enabled Opto-Electronic Learning Tools and a Supporting Framework*. Proceedings of the American Society for Engineering Education (ASEE) Annual Conference, Alburquerque, NM, 2001.

[13] D. Gupta, M. Saul, and J. Gilbertson. *Evaluation of a Deidentification Software Engine to Share Pathology Report and Clinical Documents for Research*, Informatics, American Journal of Clinical Pathology, 121: 176-186, 2004.

[14] *HIPAA (Health Insurance Portability and Accountability Act) Privacy Rule and ots Impact on Research*, http://privacyruleandresearch.nih.gov/pr_02.asp, last visited May 16, 2005.

[15] Liberty Alliance Project: Digital Identity Defined, http://www.projectliberty.org/ , last visited May 17, 2005.

[16] Macromedia E-Learning Suite 2004, http://www.macromedia.com/software/elearningsuite/ last visited May 16, 2005.

[17] Microsoft .NET Passport. www.passport.net, last visited May 17, 2005.

[18] National Center for Case Study Teaching in Science (NCCSTS), http://ublib.buffalo.edu/libraries/projects/cases/case.html , last visited May 16, 2005.

[19] The National Electronic Commerce Coordinating Council (NECCC). *Identity Management - A White Paper*, http://www.ec3.org/Downloads/2002/id_management.pdf, last visited May 16, 2005.

[20] The National Electronic Commerce Coordinating Council (NECCC) Identity Management Workgroup. *Identity Management – Are we on the same page?,* http://www.ec3.org/Downloads/2004/identity_management.pdf, last visited May 16, 2005.

[21] New NSF-AAAS report highlights 'learning communities' and other inquiry-based STEM educational strategies. Contacts G. Pinholster (AAAS) and B. Noxon (NSF), http://www4.eurekalert.org/pub_releases/2005-05/aaft-nre042905.php , May 6 2005, last visited May 17, 2005.

[22] K. Poulsen. *FBI retires its Carnivore*, SecurityFocus, Jan 14 2005, http://www.securityfocus.com/news/10307, last visited May 16, 2005.

[23] Privacy: Federal Law and Selected Court Decisions, Kansas State University, http://www.policy.ku.edu/it/privacyfederal.shtml , last visited May 10, 2005.

[24] B.Ramamurthy, S.J.Upadhyaya and R.K. Iyer. *An object-oriented testbed for the evaluation of checkpointing and recovery systems*. IEEE Int. Symposium on Fault Tolerant Computing (FTCS-27), Seattle, WA, pp. 194-203, June1997.

[25] B. Ramamurthy, *Position Paper on CS2*, Future of CS2 Workshop, presented at OOPSLA 1998, Vancouver, BC, Canada.

.

[26] B. Ramamurthy. *Industrial Training Know-how for Educators*. Workshop presented at ACM SIGCSE 2000, Austin, TX.

[27] B. Ramamurthy, and E. Crahen. *A Pedagogy to Support Modern Concepts in Distributed Systems Courses*, 2003 ASEE Annual Conference, Information Systems Track, June 23-25, Nashville, Tennessee, 2003.

[28] B. Ramamurthy et al. Collaborative: A Multi-Tier Model for Adaptation of Grid Computing to CS-based Undergraduate Curriculum, NSF Course Curriculum Laboratory and Instruction Adaptation and Implementation (CCLI A& I), award number DUE-0311473, 2003-2006.

[29] B. Ramamurthy. GridForce: Grid For Research, Collaboration and Education, invited poster at AAAS/NSF Invention and Impact Conference, Washington DC, April 16-18, 2004.

[30] B. Ramamurthy. *GridForce: A Comprehensive Model for Improving Technical Preparedness of our Workforce for the Grid*, presented at grid.edu workshop, IEEE/ACM CCGrid2004 International Conference, Chicago, IL, April 19-22, 2004.

[31] B. Ramamurthy. A Multi-tier Adaptation of Grid Computing in Computer Science Curriculum, SIGCSE 2004 poster session, Norfolk, VA, 2004.

[32] B. Ramamurthy. *Grid: The Social Imperative*, invited presentation at Erie Community College, NY, May 3, 2004.

[33] B. Ramamurthy. *Technology Culture*, invited talk, Seventh Bi-Annual Statewide Graduate School Awareness Conference for Minorities, October 9, 2004.

[34] B. Ramamurthy. Emerging Areas in Computer Science Education, invited position paper presented at a panel in CCSCE 2004, Twentieth Eastern Conference of the
Consortium of CS in Colleges, Loyola College of Maryland, Baltimore, MD, October 15-16, 2004.

[35] B. Ramamurthy. *An Overview of Grid Computing and its Adaptation to CSE Curriculum*, invited talk at SIGCSE 2005 Panel on Emerging Technologies, SIGCSE 2005, St. Louis, MO, February 2005.

[36] B. Ramamurthy. Gridforce: Grid for Collaboration and Education. http://www.cse.buffalo.edu/gridforce/index.htm, last visited May 10, 2005.

[37] B. Ramamurthy. Three *Pillars of Trust: Privacy, Identity Management and Compliance*, submitted to HICSS-39, Hawaiian International Conference on System Sciences, January 2006.

[38] Sarbanes-Oxley Act of 2002. http://www.aicpa.org/info/sarbanes_oxley_summary.htm, Last visited May 16, 2005.

[39] J. Schwartz. *FBI's Internet Wiretaps Raise Privacy Concerns New System Tracks Suspects Online*, July 12, 2000; Page A01, http://www.washingtonpost.com/ac2/wp-dyn?pagename=article&contentId=A23986-2000Jul11&notFound=true, last visited May 10, 2005.

[40] SNIP (Strategic National Implementation Process) Security and Privacy Workgroup. *De-identification on Limited Data Set*, April 2003, http://www.wedi.org/cmsUploads/pdfUpload/WhitePaper/pub/P-Final-De-identificationandLDS.pdf, Last visited May 16, 2005.

[41] SPIN/VSL Project Team. *Automated Deidentification of Pathology Reports*, Harvard Medical School, 2003, http://apiii.upmc.edu/breakout/archive/2003/balis_beckwith03/apiii-2003-Deidentification-talkx.html, last visited May 16, 2005.

[42] Sun Microsystems. *Using Identity Management to Achieve Security and Compliance*, http://www.sun.com/software/whitepapers/identity_mgmt.xml, January 2005, last visited May 10, 2005.

[43] L. Sweeney, Replacing Personally-Identifying Information in Medical Records, the Scrub System. In: Cimino, JJ, ed. Proceedings, *Journal of the American Medical Informatics Association*. Washington, DC: Hanley & Belfus, Inc, 1996:333-337, http://privacy.cs.cmu.edu/people/sweeney/scrub.html, last visited may 16, 2005.

[44] A.Thakkar and B. Ramamurthy. *Event Pipeline Pattern*, Jini Patterns Workshop, OOPSLA 2000, Minneapolis, Minnesota, October 2000.

[45] B. Thuraisingham. *Data and Applications Security: Developments and directions*, University of Texas at Dallas, Guest Lecture, April 2005, http://www.utdallas.edu/~bxt043000/Lecture27.ppt , last visited May 16, 2005.

[46] UCLA Medical Imaging Informatics (Mi^2). *Dataserver: An Open Source XML Data Gateway*, http://www.mii.ucla.edu/dataserver/docs/features/deidentification.html , last visited May 16, 2005.

[47] U.S. Department of Education. Family Educational Rights and Privacy Act (FERPA), http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html, last visited May 10, 2005.

[48] *The 2002 User Friendly Handbook for Project Evaluation,* http://www.nsf.gov/pubs/2002/nsf02057/start.htm, last visited May 16, 2005.

[1] Open Network White Papers, http://www.opennetwork.com/, last visited June 15, 2005.

[6] M. Koch and W. Wörndl: „Community Support and Identity Management“, Proc. European Conf. on Computer Supported Cooperative Work (ECSCW 2001), Bonn, Germany, Sept. 2001 http://www11.in.tum.de/publications/pdf/Koch2001a.pdf, last visited, June 15, 2005.

[7] mCrowds : Anonymity for the mobile internet, C. Andersson, S. Fischer-Hubner and R. Lundin, http://www.humanit.org/pdf/HumanIT_2003_Ch5_Andersson_et_al.pdf , last visited June 15, 2005

Privacy topic lists mostly the regulatory acts while compliance topic deals with issues in complying with privacy regulations. Identity management has been hailed as the instrument that will enable compliance with privacy rules. Thus these three form the pillars of trust in a modern electronic organization [37].