

Research creates internet privacy tool

August 24 2010

University of Arkansas at Little Rock researchers have developed a new model to manage the "vast ocean" of user-generated content being generated by the ever-growing social networking sites including Facebook and Twitter.

Dr. Nitin Agarwal, assistant professor in EIT's Department of [Information Science](#), and his doctoral student M. Venkata Swamy, worked with Dr. Srinu Ramaswamy, former chair of the UALR Computer Science Department and now vice president of research at ABB India, to develop a Context-Based [Privacy](#) Model. The model leverages intelligent, scalable, adaptive, and robust pattern-matching algorithms to allow Internet sites to automatically adjust privacy needs of consumers or organization to the context in which the data is accessed.

Their paper on the project was awarded "Best Paper" and was presented at the Second International Symposium on Privacy and Security Applications held in conjunction with the Institute of Electrical and Electronic Engineering (IEEE) International Conference on Privacy, Security, Risk, and Trust this week in Minneapolis, Minn. Only 13 percent of papers submitted at the highly competitive conference are presented.

"With the advent of social media websites such as [Facebook](#), Myspace, and [Twitter](#), and social health websites such as Patientslikeme that help people with health conditions connect with people with like conditions, a vast ocean of user-generated content has been created — including non-sensitive information as well as sensitive demographic, financial or

health-related data,” Agarwal said. “As a result, users may be unknowingly granting access to their data, leading to grave privacy concerns.”

In recent years, companies’ data information centers in industries are facing increasing federal regulations due to these [privacy concerns](#), forcing them to constantly modify their privacy information-handling policies. The existing research on developing privacy models, although seem persuasive, are essentially based on user, role or service identification. Such models are incapable of automatically adjusting privacy needs of consumers or organizations to the context in which the data is accessed.

“In this work, we propose a Context Based Privacy Model (CBPM), which leverages the automatic context identification of the information consumer borrowing concepts from Object Oriented methodology,” the researchers said. A context could be defined as a secure or non-secure location, family members, or group of friends, etc.

“Considering numerous pieces of information such as name, telephone number, e-mail address, age, gender, items purchased online, social interactions each individual generates; and the number of contexts created, the CBPM matrix could quickly become huge and unmanageable.”

The UALR team addresses that problem by leveraging intelligent, scalable, adaptive, and robust pattern-matching algorithms to compress the matrix, making it more manageable.

“Our work has shown the necessity of avant-garde privacy models dealing with the challenges of new types of information sources, creating a vast ocean of data with intricate access requirements and constraints, forcing us to think beyond the existing user, role, or service-based

privacy models,” Agarwal said. “The proposed work is unique, one of its kind emphasizing on the context more importantly than the content, with far-reaching implications in the privacy as well as the information security area.”

Provided by University of Arkansas at Little Rock

Citation: Research creates internet privacy tool (2010, August 24) retrieved 27 April 2024 from <https://phys.org/news/2010-08-internet-privacy-tool.html>

<p>This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.</p>
