

Contents

Editorial	i
Research	
Fast Remote User Authentication Scheme with Smart Card Based on Quadratic Residue- Tzong-Sun Wu, Han-Yu Lin, Ming-Lun Lee, Won-Yi Chen	51
A Refined Methodology for Automatic Keyphrase Assignment to Digital Documents- Sharifullah Khan, Iram Fatima, Rabia Irfan, Khalid Latif	55
Elementary Patterns for Converting Textual and Visual Formalisms based on Set Theory and ORM- Sietse Overbeek, Patrick van Bommel	64
Password Based Anonymous Authentication with Private Information Retrieval- Toru Nakamura, Shunsuke Inenaga, Daisuke Ikeda, Kensuke Baba, Hiroto Yasuura	72
Taxonomy-based Document Clustering- Masoud Makrehchi	79
A Practical U-Healthcare Network with Security and QoS- Shiow-Yuan Huang, Cheng-Chan Hung, Cheng-Chi Lee	87
Call for Papers	95

In this issue

Editorial

In the second issue of the year 2011, we present six valuable contributions.

The first paper addresses the smart card-based user authentication. The basic work of Lamport on remote authentication schemes, was later applied by Lu and Cao who proposed an efficient scheme based on quadratic residue. *Tzong-Sun Wu, Han-Yu Lin, Ming-Lun Lee and Won-Yi Chen* in their paper on, “*Fast Remote User Authentication Scheme with Smart Card Based on Quadratic Residue*” proposed a significant improvement to make it more efficient and secure.

Keywords are not just the labels for information and document identity, but reveal the characteristics and content of datasets. Thus, keyword identification automatically holds promise in information retrieval. *Sharifullah Khan, Iram Fatima, Rabia Irfan and Khalid Latif* in their paper on “*Refinement Methodology for Automatic Keyphrase Assignment to Digital Documents*” proposed a methodology to refine the result set of automatically generated keyphrases by Keyphrase Extraction Algorithm (KEA++), so that the keyphrases accurately and precisely represent the content of the document. They argue that their refinement methodology improves the quality of generated keyphrases.

In formal models, the exact syntax and semantics of textual formalisms reduce ambiguity and increase formulation precision. *Sietse Overbeek and Patrick van Bommel* in their paper on “*Elementary Patterns for Converting Textual and Visual Formalisms based on Set Theory and ORM*” presented patterns of ORM model of the ISO/IEC 19763-5 standard to register information of process models and later converted to a textual formal model. Besides, they converted the textual formal model of an information market to an ORM variant.

Authentication protocols are the central issue in the secure systems. *Toru Nakamura, Shunsuke Inenaga, Daisuke Ikeda, Kensuke Baba and Hiroto Yasuura* in their paper on, “*Password Based Anonymous Authentication with Private Information Retrieval*” have introduced a new set of authentication protocols that ensure the security against replay attacks and the database will not identify which user is authenticating. They have employed the Personal Information Retrieval in the core of authentication protocols and came up with strong experimental results.

Text clustering is a process in the information retrieval that has far reaching implications in detecting the required items of information in a heterogeneous cluster of unlimited volume of information. *Masoud Makrehchi* in his paper on “*Taxonomy-based Document Clustering*”, proposed a new document representation called as, the Bag-Of-Queries. With good experimentation he shown that the proposed approach outperforms bag of word based document representation for clustering. Further, he claims that it also extracts new non-redundant features and at the same time reduces dimensionality.

For ubiquitous healthcare system, the network security combined with quality of service is required to ensure integration of medical sensor platform into network environment. *Shiow-Yuan Huang, Cheng-Chan Hung and Cheng-Chi Lee* in their paper on, “*A Practical U-Healthcare Network with Security and QoS*” studied the possible security and QoS methods of a ubiquitous healthcare network platform Open System Interconnections layers. They have used the Wireless Overlay Networks (WON) Bluetooth, 802.11 and 802.16 over IPv6 Network, and provide a secure and stable U-healthcare platform by including the application of healthcare sensors with RFID, U-healthcare PDA, VoIPv6, falling detection, and patient orientation. Such an approach provides good integration for ubiquitous applications.

This issue thus offers a balanced focus on the core themes of digital information management.

Editors