THE COMPUTER JOURNAL 2014

Published by
Oxford University Press for BCS

THE COMPUTER JOURNAL is one of the longest-established journals serving all branches of the academic computer science community. It publishes high-quality papers and the latest ideas in computer science in four sections.

Section A Computer Science Theory, Methods and Tools
Section A has as its primary focus the theory and methodologies that are central to computer science. The section welcomes contributions from across this spectrum as well as papers involving the novel application of theoretical research or the adaptation of established methodologies to computational problems in other domains or within software tools. Thematic areas include but are not restricted to: algorithms and complexity; computational logic; formal methods; heuristic search; mathematics of computing; models of computation and unconventional computing; programming languages and semantics; and software engineering.

Section B Computer and Communications Networks and Systems
Section B focuses on new theories, ideas and developments in computer and communications networks and related systems. The section seeks high-quality papers reporting new concepts, architecture and experimental results in areas including but not limited to: network architectures and protocols, traffic engineering, resource management and quality of service, network monitoring and traffic measurements, wireless networks, personal and body area networks, vehicular networks, content and service-centric networking, energy efficient/green networking, opportunistic and cognitive networks, and networking in extreme/harsh environments.

Section C Computational Intelligence, Machine Learning and Data Analytics
Section C provides solutions and addresses challenging problems in such areas as data mining, image and signal processing, knowledge-based systems and the semantic web. Further thematic areas covered in this section include computational science, pattern recognition, computer vision, speech processing, machine intelligence and reasoning, web science, information retrieval, and emerging application domains in big data, e-science and u-science. It welcomes submissions with new methodology that is very extensively evaluated, and showing strong and significant results.

Section D Security in Computer Systems and Networks
The main focus of Section D is the provision of security and privacy in computer systems and networks. Contributions are welcome across all the main areas of information security and privacy, including, but not limited to: cryptography and cryptanalysis; security protocol design and analysis; intrusion detection systems and techniques; computer system security; and embedded and system security issues; user authentication techniques and systems.

THE COMPUTER JOURNAL 2014

The Computer Journal is one of the longest-established journals serving all branches of the academic computer science community. It publishes high-quality papers and the latest ideas in computer science in four sections.

Section A Computer Science Theory, Methods and Tools
Section A has as its primary focus the theory and methodologies that are central to computer science. The section welcomes contributions from across this spectrum as well as papers involving the novel application of theoretical research or the adaptation of established methodologies to computational problems in other domains or within software tools. Thematic areas include but are not restricted to: algorithms and complexity; computational logic; formal methods; heuristic search; mathematics of computing; models of computation and unconventional computing; programming languages and semantics; and software engineering.

Section B Computer and Communications Networks and Systems
Section B focuses on new theories, ideas and developments in computer and communications networks and related systems. The section seeks high-quality papers reporting new concepts, architecture and experimental results in areas including but not limited to: network architectures and protocols, traffic engineering, resource management and quality of service, network monitoring and traffic measurements, wireless networks, personal and body area networks, vehicular networks, content and service-centric networking, energy efficient/green networking, opportunistic and cognitive networks, and networking in extreme/harsh environments.

Section C Computational Intelligence, Machine Learning and Data Analytics
Section C provides solutions and addresses challenging problems in such areas as data mining, image and signal processing, knowledge-based systems and the semantic web. Further thematic areas covered in this section include computational science, pattern recognition, computer vision, speech processing, machine intelligence and reasoning, web science, information retrieval, and emerging application domains in big data, e-science and u-science. It welcomes submissions with new methodology that is very extensively evaluated, and showing strong and significant results.

Section D Security in Computer Systems and Networks
The main focus of Section D is the provision of security and privacy in computer systems and networks. Contributions are welcome across all the main areas of information security and privacy, including, but not limited to: cryptography and cryptanalysis; security protocol design and analysis; intrusion detection systems and techniques; computer system security; and embedded and system security issues; user authentication techniques and systems.
CONTENTS

ORIGINAL ARTICLES

481 Server-Aided Signature Verification for Lightweight Devices
Fuchun Guo, Yi Mu, Willy Susilo and Vijay Varadharajan

494 ZIDS: A Privacy-Preserving Intrusion Detection System Using Secure
Two-Party Computation Protocols
Salman Niksefat, Babak Sadeghiyan, Payman Mohassel and Saeed Sadeghian

510 Forward-Secure Hierarchical Predicate Encryption
Juan Manuel González Nieto, Mark Manulis and Dongdong Sun

537 Detecting Distributed Denial of Service Attacks: Methods, Tools and Future Directions
Monowar H. Bhuyan, H. J. Kashyap, D. K. Bhattacharyya and J. K. Kalita

557 Adaptive ±1 Steganography in Extended Noisy Region
Tao Han, Weiming Zhang, Chao Wang, Nenghai Yu and Yuefei Zhu

567 A New Framework for Conditionally Anonymous Ring Signature
Shengke Zeng and Shaoquan Jiang

579 Attribute-Based Data Transfer with Filtering Scheme in Cloud Computing
Jinguang Han, Willy Susilo, Y. Mu and Jun Yan

592 Efficient Revocable Certificateless Encryption Secure in the Standard Model
Limin Shen, Futai Zhang and Yinxia Sun

602 MLH-IDS: A Multi-Level Hybrid Intrusion Detection Method
Prasanta Gogoi, D.K. Bhattacharyya, B. Borah and Jugal K. Kalita

624 Achieving Key Privacy and Invisibility for Unattended Wireless Sensor Networks in Healthcare
Faeezeh Sadat Babamir and Ali Norouzi

636 Insecurity of ‘Improved Anonymous Multi-Receiver Identity-Based Encryption’
Huaqun Wang