Guest Editors' Introduction

Leading-Edge Technologies

Rick Kuhn
National Institute of Standards and Technology

Samee U. Khan
North Dakota State Universty

It usually seems that the pace of change in computing is ever-increasing. A quasi-formal statement of this progress is of course Moore's Law. Originally, an empirical observation was that the number of transistors in an integrated circuit doubles roughly every two years; this observation is now often a general expression of the exponential rate of progress in information technology (IT).

For the past few decades, IT progress has been primarily in the speed and capacity of processors and data storage, but qualitative changes are happening as well—and these changes are moving rapidly into the consumer space. "Self-driving" cars are the talk of the automotive industry, and intelligent assistants such as Amazon's Alexa and Apple's Siri are incorporated into everyday life in cell phones and voice-response units for the home. These advances have been made possible by enormous advances in hardware and software, but they in turn are triggering a need for even greater improvements. We now depend on the safety, reliability, and security of computing systems in areas that used to be solely the domain of human workers.

Staying on top of these changes is a real challenge for IT professionals, who require a deeper understanding that may be needed to integrate advanced capabilities in large mission-oriented systems. In this issue, we take a look at some important new technologies for IT systems, cognitive computing and autonomous control, and also at fundamental advances in quantum computing that may enable even more remarkable achievements.

Digital Object Identifier 10.1109/MITP.2019.2947990
Date of current version 6 November 2019.

In "Autonomous Cars: Challenges and Opportunities," the authors have done a fantastic job in providing a short description of the state of the art of autonomous cars—predominantly focusing on the stakeholders of autonomous vehicles, e.g., vehicle manufacturers, insurers, legislators and regulators, and transportation infrastructure managers. The work also reports various aspects related to autonomous vehicles manufacturing and development, such as terms and definitions, autonomy models, technological aspects, and applications of the autonomous vehicles. The work concludes with the listing of some very important challenges in the domain of autonomous vehicles. The work will certainly resonate with IT practitioners interested in works related to autonomy within the context of autonomous vehicles.

In "The Adoption of Cognitive Computing Technology in China," Linda Lai provides the current landscape of the adoption of cognitive computing in China. As defined by Lai, cognitive computing integrates various data sources, algorithms, and other methodologies to mimic human cognition to resolve a set of problems. Lai has done a fantastic job in providing a history of the domain in China with some hard evidence (reference to economic impact and China Five-Year Plans). Lai was also able to provide a perspective of how China's efforts stack up against other nations. Lai also provides significant details on how these efforts are moving various fields in China forward, such as health care, education, energy, and business. Finally, Lai ends her reporting with some opportunities to consider in cognitive computing—moving forward, such as security and privacy.

1520-9202 © 2019 IEEE
Published by the IEEE Computer Society

Quantum computing is among the most exciting developments in computer science and engineering of the past two decades, because of its potential to provide exponentially faster processing for certain applications. In "Design of Quantum Computing Circuits," the authors provide a basic introduction to this fascinating field. They introduce the basic concepts of quantum computation, followed by an explanation of reversible logic gates for quantum circuit design. To show how these concepts are used in computing, they describe the design of quantum circuits for addition, subtraction, conditional addition, and multiplication, basic components out of which more complex computations can be developed.

Quantum computation opens the door to many opportunities for high-performance computing, but in so doing, it presents a new challenge. Existing public-key cryptographic algorithms are all vulnerable to attack by quantum computing, when a practical quantum computer is developed. To prepare for this eventuality, researchers have developed a wide range of approaches to "post-quantum cryptography," i.e., cryptographic algorithms that cannot be easily broken with quantum computing. The article "Isogeny-Based Cryptography: A Promising Post-Quantum Technique" presents an example of one such method. This article provides an introduction to both the challenges of post-quantum cryptography and a potential solution. The authors introduce the basics of elliptic curve methods, and then show how they can be used to design the hard problems that can provide a basis for quantum-resistant cryptography.

We hope the reader will both enjoy and be inspired by the exciting changes presented in these articles, and possibly imagine new ways to use these in systems that will benefit the world.

ACKNOWLEDGMENT

The work of Samee U. Khan was supported by (while serving at) the National Science Foundation (NSF). Any opinion, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the NSF.

Rick Kuhn is a computer scientist in the Computer Security Division of the National Institute of Standards and Technology, and is a Fellow of IEEE. Contact him at: samee.khan@ndsu.edu.

Samee U. Khan is a professor at the ND State University from where he is on leave to serve at the National Science Foundation. He is an ACM Distinguished Speaker and an IEEE Distinguished Lecturer.

IEEE Computer Society Has You Covered!

WORLD-CLASS CONFERENCES — 200+ globally recognized conferences.

DIGITAL LIBRARY — Over 700k articles covering world-class peer-reviewed content.

CALLS FOR PAPERS — Write and present your ground-breaking accomplishments.

EDUCATION — Strengthen your resume with the IEEE Computer Society Course Catalog.

ADVANCE YOUR CAREER — Search new positions in the IEEE Computer Society Jobs Board.

NETWORK — Make connections in local Region, Section, and Chapter activities.

Explore all of the member benefits at www.computer.org today!

IEEE COMPUTER SOCIETY

IEEE