Opportunities and Obligations for Physical Computing Systems
pp. 23-31
John A. Stankovic, Insup Lee, Aloysius Mok, and Raj Rajkumar

The authors envision data and services that will be available any place, any time, to all people. Major systems such as those in transportation, manufacturing, infrastructure protection, process control, and electricity distribution networks will become more efficient and capable. People will be safer and experience an improved standard of living. New applications not even imagined today will become a reality.

Although ingredients of this vision have existed for several years, the authors believe that developers must focus on the physical, real-time, and embedded aspects of pervasive computing. They refer to this domain as physical computing systems. For pervasive computing to achieve its promise, developers must create not only high-level system software and application solutions, but also low-level embedded systems solutions.

Heterogeneous Chip Multiprocessors
pp. 32-38
Rakesh Kumar, Dean M. Tullsen, Norman P. Jouppi, and Parthasarathy Ranganathan

Chip multiprocessors have recently expanded from an active area of research to a hot product area. If Moore’s law continues to apply in the chip multiprocessor era, we can expect to see a geometrically increasing number of cores with each advance in feature size.

A critical question in CMPs is the size and strength of the replicated core. Many server applications focus primarily on throughput per cost and power. In reality, application needs are not always so simply characterized, and many types of applications can benefit from either the speed of a large core or the efficiency of a small core. Thus, the authors believe the best choice in core complexity is a heterogeneous chip microprocessor with both high- and low-complexity cores.

High-Performance, Power-Aware Distributed Computing for Scientific Applications
pp. 40-47
Kirk W. Cameron, Rong Ge, and Xizhou Feng

The evolving parallel and distributed systems designed for demanding scientific simulations will be enormously complex and power hungry. Computers capable of executing one trillion floating-point operations per second have already emerged, and petaflops systems that can execute one quadrillion floating-point operations per second are expected by the end of the decade.

Because supercomputing experts cannot agree on what the core technologies should be, these systems will likely be diverse as well. Nevertheless, most will be built from commercial components in integrated scalable clusters of symmetric multiprocessors. Such solutions will be highly parallel, with tens of thousands of CPUs, tera- or petabytes of main memory, and tens of Pbytes of storage. Advanced software will synchronize computation and communication among multiple operating systems and thousands of components.

Battery Sensing for Energy-Aware System Design
pp. 48-54
Roberto Casas and Oscar Casas

As portable electronic devices become ever more useful, developers have begun to envision rich pervasive computing environments and instrumentation systems in the form of wireless sensor networks. Unfortunately, energy supply and storage technology are not advancing at the same rate. Whereas computer processor speed and memory capacity have exhibited an orders-of-magnitude increase since the 1990s, battery energy density has only tripled.

Making these devices function properly and for as long as possible using only limited power resources has become critical. Research on state-of-charge, or the remaining energy in the batteries, is of key importance. Whereas previous work on battery modeling described how to model batteries using parameterized state-of-charge measurements, the authors propose commercial devices for each parameter that designers can adopt in real applications where fuel gauging is needed.

A Scientific Approach to Cyberattack Detection
pp. 55-61
Nong Ye and Toni Farley

Despite many attempts to counter them, cyberattacks on computer and network systems continue to threaten the global information infrastructure, targeting data files, services, or service ports. Unfortunately, current countering methods—prevention, detection, or reaction—tend to be inefficient, inaccurate, and limited.

Developers of detection systems, in particular, tend to rely on empiricism or heuristics, a strategy that lacks a deep scientific understanding of the signals an attack can give off in cyberspace. The inadequacies of the two most recognizable attack-detection approaches—signature recognition and anomaly detection—are a case in point.

Given these gaps in detection accuracy, perhaps it is time to look at more scientific principles, such as those embodied in established signal-detection models that are adept at handling a mix of signal and noise data. With such models, it might be possible to separate attack and norm characteristics, permitting the least amount of relevant data to detect a wide range of attacks accurately and efficiently.

Robust systems with the scientific and engineering rigor of signal-detection technologies would offer a deep understanding of signal and noise characteristics. This knowledge in turn might make it possible to build mathematical or statistical models that can accurately detect an attack signal in a sea of normal-use activity even if the attack is subtle.