Wearables, Implants, and Internet of Things: The Technology Needs in the Evolving Landscape

Sandip Ray, *Senior Member, IEEE*, Jongsun Park, *Senior Member, IEEE*, and Swarup Bhunia, *Senior Member, IEEE*

Abstract—The proliferation of wearable and implantable computing devices in the recent years, and the emergence of the Internet of Things, have ushered in an era of computing characterized by an explosion in growth and diversification of computing platforms. Unfortunately, the traditional research silos in computing science and engineering appear inadequate for enabling and sustaining the requirements of this new computing era. This paper examines some of these key requirements, explains why the current computing abstractions and research silos are insufficient, and identifies several research challenges. The challenges cross-cut several computing disciplines, including programming languages, computer architecture, physical designs, security, algorithms, and analytics.

Index Terms—Security, privacy, Internet of Things, implants, wearables, analytics, ultra low-power, authentication, connectivity

1 Introduction

Even a few years back, computing systems could be clearly categorized into two categories: (1) *general-purpose computing systems*, including desktops, laptops, and servers, and (2) *embedded systems* for customized applications, e.g., biomedical, traffic control, etc. The categorization made sense since there was a clear demarcation between the two categories from the perspectives of application and design/development. General-purpose computing was characterized by a standardized—albeit complex—instruction set architecture, high programmability, decoupling of software applications from the underlying hardware platform, and the ability to support diverse use-cases. Embedded system designs were tailored towards meeting the potentially unique use-case constraints of target applications and also featured tight hardware/software integration. This categorization was challenged by the advent of programmable, hand-held computing devices like smartphones and tablets. These designs required the high programmability, standardization, and support for diverse use-cases on the one hand, and customization for unique form factors, use-case constraints, and hardware/software integration on the other. The ability to perform with small, mobile devices, the scale of computing that required high-end systems of a decade back has, in turn, revolutionized the use-cases themselves. For example, we now routinely use smartphone devices for personal and intimate applications including tracking our sleep and physical fitness, helping with directions, capturing and editing pictures and videos, etc.—activities that earlier required separate and unique embedded devices. The paradigm shift has been so great, that the very definition of an embedded system has changed over the last decade from "a system intended to provide a dedicated function" [1] to "any computing device that is not a desktop, laptop, or server" [2].

As we continue the trend of rapid miniaturization of computing technology and develop computing devices of increasing speed with small form factors and low power, we are standing today on the verge of yet another revolution in computing paradigm, a world of implants, wearables, and Internet of Things (IoT). This world represents a shift from personalized, individual phones and tablets towards tens of billions of small, smart, connected devices either deployed on-field or implanted or worn by humans and animals, performing computation through a coordinated interaction through a cloud of servers and data-centers. The "tens of billions" above is not a figure of speech: the number of connected computing devices is projected to reach 50B by the year 2020 from a "mere" 2B in 2005—a faster rate of growth in number and diversity than any consumer commodity market [3]. The dramatic effect of this explosion is most striking in the scale of the computing applications being pursued. Two decades back, today's versatile smartphones represented the boundary of expectation from computing devices that a reasonably savvy individual could imagine. Today, we not only imagine but have already realized applications of the scale of smart *cities*!

Given this extreme diversification of computing platforms, we are also on the verge of new challenges for technology to support the diversification. Interestingly, the trend in this new technology is towards *unification* of ideas from areas of computer science, engineering, and information technology, which had so far maintained an identity of separation and isolation. These include areas as diverse as computer architecture, hardware/software co-design, security, physical planning and layout, verification, and analytics, among many

- *S. Ray is with the Strategic CAD Labs, Intel Corporation, Hillsboro, OR 97124. E-mail: sandip.ray@intel.com.*
- *J. Park is with the School of Electrical Engineering, Korea University, Korea. E-mail: jongsun@korea.ac.kr.*
- *S. Bhunia is with the Department of Electrical and Computer Engineering, University of Florida, Gainesville, FL 32611. E-mail: swarup@ece.ufl.edu.*

Manuscript received 20 Oct. 2015; revised 20 Mar. 2016; accepted 22 Mar. 2016. Date of publication 11 Apr. 2016; date of current version 21 July 2016. Recommended for acceptance by P.P. Pande.
For information on obtaining reprints of this article, please send e-mail to: reprints@ieee.org, and reference the Digital Object Identifier below.
Digital Object Identifier no. 10.1109/TMSCS.2016.2553026

others. In this new world, there are clear indications that these areas will progress through cross-fertilization and collaboration, perhaps even completely blending with one another to the point that many of the isolated existences may become indiscernible.

In this paper, we lay out a vision and perspective of the world of wearables, implants, and IoT devices from the point of view of technology unification. We discuss the technology needs for enabling the device and platform explosion, identify the deficiencies of some of the currently established technology silos, and discuss how these deficiencies can be alleviated through collaboration. In the process, we identify several research topics at the cross-roads of the different areas in computer science, engineering, and information technology.

The remainder of the paper is organized as follows. Section 2, 3, and 4 briefly recount the history and current state of wearables, implants, and IoTs. The three sections are not intended to be comprehensive surveys of these highly diverse areas, but rather to set the background for discussing the emerging technology challenges. Section 5 identifies some key requirements in the new world from the perspective of end-user experience expectation. In Section 6, we examine some of the critical new technology challenges that must be addressed to make such user expectation a reality. We conclude in Section 7 by making the case that breakthrough innovation in the new world today requires collaborative effort breaking the boundaries of individual topic areas.

2 Wearables

Wearable computers are loosely characterized as computing devices that can be operated *naturally* and *effortlessly* by the human when worn. The requirements of natural and effortless operation distinguishes a wearable computing device from a portable one such as a small laptop or tablet. Wearable devices are also expected to run continuously for long periods without need for human intervention.

Depending on what counts as a "computing device", the history of wearable computers arguably dates to the abacus ring of the 1,600s. One of the first instances of a prototype wearable device making use of the modern computing technology was the Thorp timing device [4], introduced to help cheat in a game of roulette. It made use of switches to estimate speed of the roulette wheel and provided output in the form of a musical note to a miniature radio hidden in the ear-canal of a collaborator. The rise in computing power during 1980s and 1990s saw increasing sophistication and diversification in wearable form factors and applications. Examples of wearable form-factors for general-purpose computing at this time included the VuMan system from Carnegie Mellon University, the Columbia University KARMA system, the University of Toronto "wrist computer", among others.

One of the first commercial wearable devices was the *Private Eye* head-mounted display, which scanned a vertical array of LEDs across the visual field. The Private Eye was subsequently augmented to a virtual reality wearable eyeglass. With advancing sensor technology, advent and standardization of wireless connectivity paradigms, and improving power/performance of computing devices, the number and diversity of wearable form factors has exploded over the last decade. Wearable computing has made successful and significant forays in fitness domains, health care, fashion, and entertainment. In particular, we now routinely use commercial fitness trackers in the form of arm bands and smart watches. Computing devices are getting woven into textiles to provide added value to our clothing. Wearable devices today are trending towards more general-purpose applications to provide a holistic user experience. For example, current smart watches provide not only a fitness tracking functionality but also email and calendar notifications; smart earbuds permit the user to track heart rate while listening to music in a workout; virtual reality has made a comeback with commercial VR headsets providing an immersive user experience of augmented reality; smart eyeglasses such as Google glass is intended as a basis for a hands-free, mobile, general-purpose computing device supporting diverse third-party applications.

3 Implants

Implantable systems typically interface with internal body parts to record and/or manipulate biological activity for diagnostic or therapeutic purposes. Analogous to wearable devices, implants must be small and capable of performing independently without user intervention (and replacement). Unlike other miniaturized computing devices, however, installation of implants has traditionally involved an invasive procedure; consequently their usages have obviously been restricted until recently to usage scenarios where potential benefits could justify the associated risk. A quintessential usage of implants for humans has been for treating serious medical conditions. More recently, with sophistication and miniaturization of computing and process technologies, the scope of implants is expanding to areas such as fitness, fashions, etc. Because of their invasive nature and potentially direct interaction with human biology, a critical challenge is for these devices to be certifiable for security, reliability, and execution correctness to more exacting standards than has been typically provided for traditional computing systems.[1]

One of the earliest medical implants was the implantable pacemaker which was successfully inserted into a human in 1960 [5]. Some other early implantable medical devices have included defibrillators for monitoring and treating cardiac conditions, neurostimulators for deep brain stimulation for patients with epilepsy or Parkinson's disease, infusion pumps for drug delivery, etc. More recently, biomedical implants have been used as a proactive medical device to automatically monitor the health of internal organs and provide early detection mechanism (*i.e.*, before symptoms arise) of targeted health conditions such as systemic inflammatory response, stenosis, and tumor.

Aside of the use in medical cure and monitoring, implants have also found use as means for personalized data acquisition and actuarial activities. Microchip implants are IC devices or RFID transponders implanted in the body of a human being or an animal, typically underneath the

1. Computers have been used for sensitive application for decades, ranging from banking, shopping, military, and indeed, medicine and biomedical applications, and these devices have indeed required significantly higher evaluation standards than a traditional desktop or laptop. However, the difference between such safety-critical systems of the past and the emergent implants and wearables is the increaqsing complexity, which makes such certification challenging.

skin. Such implants typically contain a unique identification number and can be connected to an external database. These implants are commonly employed on animals, e.g., to identify farm and ranch animals, track members of endangered specifies, etc. More recently they are also being used with humans e.g., for personal identification, medical history, medications, etc.

These systems can largely benefit from *in-situ* real-time signal processing. Such signal processing typically serves two major purposes: (1) compression of recorded data; and (2) real-time online signal analysis in order to recognize meaningful patterns from recorded data. Data compression is an important requirement for systems, which wirelessly transmit recorded signal to the external world, possibly from multiple channels, in order to drastically reduce transmission bandwidth and energy requirements. On the other hand, pattern recognition from recorded data is important in closed-loop implantable systems for manipulation of body activity or drug delivery [6]. With increasing requirements of the implantable and wearable systems to perform advanced digital signal processing (DSP) on large volume recorded data, there is a growing need to develop efficient signal processing algorithms along with their low-power, low-area hardware implementation [7].

4 Internet of Things

The wearables and implant technologies above, while expanding and generalizing significantly in recent years are still somewhat enclosed in terms of application, form factor, and design. The Internet of Things, however, is one of the most general paradigms of smart, connected devices. It is beyond the scope of this paper to go into depth on all aspects of IoT, and the curious reader is referred to a recent tutorial [8] for a more thorough treatment. In its general form, IoT is simply a network of physical objects or "things" with attached software, sensors, and network connectivity, permitting these objects to exchange data. An IoT infrastructure includes three components: (1) a collection of low-power *edge devices* receiving sensory data from the physical objects and controlling responses to these objects, (2) a network of routers and possibly gateways for communication and propagation, and (3) a *cloud* of servers and data centers to store data and perform computation-intensive processing.

As a concept, the notion of smart, connected devices has a long history. One of the first instantiations of a "thing" connected to the Internet was a modified soda machine at the Carnegie Mellon University in 1982, which could report its drinks inventory as well as the temperature of the drinks stored [9]. In the 1990s, significant progress was made by papers from Weiser [10] and Raji [11] that created the vision of smart connected devices across consumer and enterprise sectors. In the 2000s, two other factors were added to the equation: accessibility of continuous Internet connectivity, and the rise and popularity of mobile devices such as smartphones and tablets. Consequently, it became possible to write applications on mobile devices that could communicate, direct, and guide sensor-controlled devices. Today we are witnessing increasingly smarter sensor devices with highly sophisticated applications. Current commercial consumer services based on IoT devices include comprehensive home security systems, smart thermostats with remote monitoring, etc. Emerging applications include smart and energy-efficient homes, shopping complexes, even cities; communication and management of transportation [12]; and monitoring and management of environment [13].

5 User Expectation in the New World

To understand the technology needs in the emerging world of wearables, implants, and Internet of Things, a first step is to anticipate the expectation of the user from the computing device in this world. Unfortunately, such anticipation is bound to be speculative. Nevertheless, the present can provide some indication of the trend, which can be based on a reliable predictor for the short to medium-term future. Based on the current applications, the following three key trends appear in terms of user expectation of computing experience.

Intelligent devices. Smartness is the first overarching requirements of computing devices. We are already in the world of smartphones, smart watches, and looking to a future with increasingly complex and intelligent applications. It may be worth reflecting upon what can make computing devices qualify to be smart. A smart device is primarily one that is aware of the *context* in which it receives information from sensors and automatically derives the appropriate response for that context [8]. As we move towards the future, we can speculate that smartness will be increasingly defined by awareness and response to the environment. A smart computing application will anticipate the *context*, learn from it, and adapt to the user needs. It is worth noting that the context itself is not static: it changes along the time of day, days of the week, seasons of the year, and age of the people. For instance, a smart home energy management system must understand how to adjust the ambient lights in the rooms of different residents in the evenings versus mornings, in summer versus winters, when working versus listening to music, when they are euphoric versus depressed, etc. This data comes from a large number of sensory devices aggregated over time, with fluctuations and random variations, possibly from analysis of behavior patterns of a large number of similar people. Furthermore, the "perfect" lighting for the mood may not be the ultimate objective: it has to be balanced against considerations such as energy efficiency requirements, security and privacy concerns in data gathering (see below).

Continuous connectivity. Imagine a future of self-driving cars that coordinate with one another in a busy highway; a connectivity loss can become a catastrophe. Connectivity is important even for less dramatic applications: a smart coffee machine failing to provide the user a notification at the time the coffee is ready (or even providing a significantly delayed response) is not fitting for a smart device. Users in the new world expect applications to provide real-time responses with respect to human response time. Indeed, connectivity is the critical backbone of the new world—it is what permits devices to perform immersive user experiences, react to changes in the physical environment, and indeed makes the Internet of Things possible. But connectivity is not merely a device-to-device connection—it also includes a collaboration between the device and the human. Devices must seamlessly connect to the physical world, obtain and detect sensor

information, propagate them to the human when needed even when the human is on the other side of the world, and react instantaneously to human requests. However, connectivity is a highly complex, heterogeneous mechanism; edge devices connect locally to others through a local network that connects to clouds and datacenters through routers and gateways. Each of these systems work on different network protocols, and each includes devices which can fail unpredictably. Connectivity entails ensuring that an application with billions of possibly faulty (even malicious) devices can provide the user with a view of continuous, coordinated communication.

Security and privacy. The smartness and connectivity requirements above emphasize the coordination and cooperation among computing devices. Security, on the other hand, provides a sobering trade-off. As discussed above, a smart device must—of necessity—understand and analyze behavior patterns, moods, and expectations of the user. This is only possible by access to personal, private, information about the user, e.g., a smart fitness tracker has access to such intimate details as kind and quality of sleep, heart rates, etc. As we move towards aggregating and consolidating more and more personalized information, it is critical to ensure that the data remains secure and free from malicious access. With emergence of new IoT systems, security becomes a critical issue both because of the large diversity of connected systems and the "globalization" of the information storage and aggregation locations. First, with billions of connected devices, it is possible for one rogue or compromised device to make the entire system vulnerable. Second, data is aggregated and stored in datacenters and cloud instead of a personal desktop or laptop; it is unclear how or whether such data can be compromised, who has access to it, etc. [14], [15], [16]. Indeed, if a goal of smartness is making data collection transparent to the user to provide an immersive experience, that comes in direct conflict with the requirement that the user must understand when (and to whom) personal details are being divulged.

6 Technology Challenges

What kind of technology challenges do we need to overcome to make the world of billions of smart, connected, communicating devices providing for a holistic, immersive, and secure user experience? Here we outline a few critical ones. The description below should be taken as merely providing a flavor of the scale and diversity of technical challenges, not as a comprehensive list.

Power and energy efficiency. A fundamental requirement for wearables, implants, as well as IoT edge devices, is to work with little energy consumption. For example, a battery-operated thermostat that wakes up once every few minutes to check the temperature and adjust the air-conditioning based on its findings needs to consume as little power as possible to minimize battery replacement. With billions of devices performing in an "always-on" mode, the low-power requirement is critical to ensure that energy consumption of the devices themselves does not subvert the overall application motivations of smart, energy-efficient buildings, cities, or environment. Of course, low-power requirements are not specifically new for sensor devices. However, the requirement gets challenging since emerging computing devices are not "just" sensor devices; they must perform sophisticated computation, coordinate with other devices in the vicinity, collect and aggregate data for propagation to the cloud, and respond in real time to user requests or application responses.

For implants, ultra-low power operation is essential in order to enable long-term operation using the embedded battery. Even with rechargeable batteries enabled by inductive charging, it is important to reduce power dissipation to increase the battery lifetime. Besides, low-power operation is also important to avoid tissue damage due to power-density induced temperature rise. Prior research efforts have shown that the power issue in implant can be addressed in efficient manner by exploiting the nature of data and/or the signal processing algorithms under consideration, instead of using conventional design techniques [17], [18].

Another important design requirement for implementing signal processing algorithms in these systems is *reconfigurability* that enables tuning functionality during deployment. For example, in case of implants, variations in the nature of biological signals for different subjects as well as temporal variations in signal and noise characteristics require calibration and tuning of the various parameters or changing functionality. To achieve this, one can use software configurability, where the algorithm is coded in an embedded microprocessor. However, compared to a custom implementation, this can incur large overhead in terms of area and power requirements. An alternative is to consider hardware reconfigurable platforms such as Field Programmable Gate Array (FPGA).

However, existing FPGA systems are often beyond the area and power budget allowable by implants and many IoT systems. This necessitates the investigation of alternative hardware reconfigurable architectures such as Memory Based Computing (MBC) [19]—a spatio-temporal architecture, which can be used to implement a particular algorithm within the area, power and performance bound. It keeps the option of reconfigurability in order to achieve the flexibility of in-field alterations. Such a reconfigurable computing framework uses a dense memory array as underlying computing element, leading to significant power reduction at iso-performance compared to state-of-the-art FPGA [19]. In order to satisfy the area and power constraints, one can use a judicious mix of reconfigurable memory-based computing and custom logic blocks which can give us the required adaptability. Again, it is worth utilizing the application properties to perform this division. Another possibility is to use multi-mode systems, which can be configured into limited well-defined modes, while providing ASIC-like performance and energy-efficiency [20].

Security. We touched upon security challenges while discussing user expectations on security and privacy in the preceding section. The key challenge in privacy is to ensure that user privacy is respected in an accountable manner while still permitting transmission and aggregation of sufficient user information to permit personalized user experience. However, end-user privacy is only one vector of the security requirement. Devices, by their very design, contain other security assets from manufacturers and content providers, e.g., firmware, cryptographic keys, DRM keys, etc., which must also be protected. However, access to all these assets

are governed by complex security policies, which may themselves be upgradable on-field. For example, a device initially launched into field may have its DRM keys locked. Subsequently, policies may change either because of the need to remotely patch DRM (which may involve giving temporary access the DRM keys through some debug port), or the DRM may become open if the content provider agrees to provide free unlimited access. The device therefore must permit facilities for secure lock while allowing for a potential upgrade to unlock under various constraints. Finally, the communication to upgrade a key or firmware itself has to happen remotely, potentially through routers and gateways which can be rogue or compromised. A key challenge then is to ensure that it is still possible to reliably enforce upgrades, patches, and modifications to individual devices.

With pervasive use of implantable systems and increasing need for wireless transmission of the sensed data, these systems are being increasingly vulnerable to diverse attacks by adversaries, who can potentially snoop/manipulate the sensed data or control signals. Hence, it is becoming important to protect the recorded data and control signals in wireless implantable systems. However, such protection needs to come at extremely low power and area overhead. Conventional data encryption solutions consume too much power and require too large silicon area to be effectively used in implantable systems. Hence, there is an emerging need for efficient low-overhead data protection approaches for these systems. Because biological signals are subject to some intrinsic random variations, low-cost key-based obfuscation techniques that exploit the nature of the recorded biological signal can provide required data protection while still operating at ultralow power budget [18]. Such an approach scrambles the data at multiple levels using separate secret keys and requires minimal extra hardware.

Analytics. Data mining is one of the backbones of the new digital world. Sensor information—the raw data from edge devices—is useless on its own: it is analytics that creates information out of this raw data and helps create an infrastructure in which the computing application can respond to the user requests or even anticipate user needs and desires. However, data analytics comes with its challenges. We saw one of them already in the context of security: how to obtain sufficient, relevant data without compromising the user's privacy and security requirements. Another critical challenge is to identify how much data to collect, and how to aggregate them in a manageable manner. Note that the continuous stream of raw sensor data from billions of devices, if transmitted directly to the cloud for processing, would overwhelm the bandwidth of the Internet and the processing ability of data centers. It is critical to perform staged aggregation of this data, at the edge, at the routers, at the gateway, and at the cloud. Finally, the "cloud" itself is not a single computing entity but a distributed network of servers; it is critical to identify ways to partition data mining tasks within this network, and distributed techniques for machine learning and analytics.

Software development. It is important to note that the "raw" hardware of any computing device does not satisfy any of the requirements of smart, connected, holistic user experience. Hardware components manipulate low-level signals, and can suffer from electrical glitches and noise. Consequently, IoT applications squarely depend on software developers to turn the hardware into an intelligent, immersive application. Software developers of IoT systems include (1) developers working directly with low-level devices and sensors, (2) developers working on telemetry and data mining for useful information from sensor data, and (3) front-end developers writing high-level applications. The skills and infrastructure requirements for each of these categories have little commonality. Consequently, development along the different vectors often happens at cross-purposes, often with no single common language, infrastructure, or metric for developing an end-to-end solution. Solving this requires a new software development paradigm, and possibly a new breed of software developers that has overall familiarity, if not expertise, in the overall scope of the application from device to cloud.

Aggressive timeline. In the world of desktops and laptops, the standard design life-cycle from exploration to production was about 3-4 years. In the world of wearables, this time interval is expected to shrink to a few months. How can we develop smart, highly complex devices with a myriad of form factors within this short time window? The obvious answer is, of course, reusability of designs, platforms, implementations, and development between one device and another. However, this is a serious challenge for small, smart, mobile devices precisely because they are typically targeted towards specific applications. For instance, a device targeted for tracking user fitness would involve significantly different design choices, security requirements, and power profile than a device to be installed in a smart car. The challenge then is to develop a standardized infrastructure or "skeleton" for building devices that enable reusability while still permitting fast customization for individual applications.

7 An Argument for Breaking the Walls

To emphasize the role of collaboration and joint investigation for a viable solution in the IoT space, let us take the example of data analytics challenge from the previous section. Traditional data mining techniques have focused on the quality of data and classification/inference techniques to glean effective information from that data. However, in the emergent world, such a view is not adequate. One must account for how the data is collected, whether security issues cause certain critical pieces of data to be unavailable (and how to circumvent that problem while still providing effective user experience), how much power may be consumed to gather the necessary data, how complex it may be to propagate it to the cloud, how to distribute analytic requirements to gateways, routers, and edges (each operating under a different power profile), etc. Clearly, solving this problem requires a deep understanding of not only analytics but security, distributed computation, performance and energy models, etc.

The story is similar for providing any end-to-end solution in the new world. Smartness, on its own, requires understanding of human-computer interactions as well as the limits of computing ability under the constraints of data and energy limitations. Connectivity requires understanding how much one can tolerate device failures while still providing a smooth, seamless experience of a smart device. Security requires

understanding the functionality requirements so that security constraints do not turn the application into a "piece of brick" while still providing the necessary trustworthiness.

This state of the affairs is a challenge for research. Research thrives on abstractions that permit one to continue investigation in a specific area without significant concern over the research challenges in all the other areas that it touches. In modern microprocessors, instruction set architectures and programming languages provide an abstraction that permit software developers to develop applications without requiring deep knowledge of the underlying hardware implementations and optimizations. The fact that we cannot create similar silos for these new, emerging applications perhaps suggests the relative youth of the topic. We are merely scratching the surface of these new devices and technologies, groping, probing, and understanding how to systematically explore this space. We hope that by collaboration among researchers and practitioners at different aspects of this new regime can we hope to finally develop those critical abstractions that permit deeper exploration of independent silos.

Acknowledgments

The work is supported in part by US National Science Foundation (NSF) Grants 1603475, 1603480, and 1603483, and Semiconductor Research Corporation grants 2015-EP-2650 and 2651.001.

References

[1] S. Heath, *Embedded Systems Design* (EDN Series for Design Engineers), 2nd ed. Oxford, U.K.: Newnes, 2002.
[2] "Embedded Systems," in *PC Mag.*, 2012, http://www.pcmag.com/encyclopedia/term/42554/embedded-system
[3] D. Evans, "The internet of things: How the next evolution of the internet is changing everything," [Online]. Available: http://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf, Accessed Apr. 21, 2016.
[4] E. Thorp, "The invention of the first wearable computer," in *Proc. 2nd Int. Symp. Wearable Comput.*, 1998, pp. 4–8.
[5] S. Furman and J. Schewedel, "An intracardiac pacemaker for stokes-adams seizures," *N. England J. Med.*, vol. 261, no. 5, pp. 943–948, 1959.
[6] M. A. Nicolelis, "Actions from thoughts," *Nature*, vol. 409, no. 6818, pp. 403–407, 2001.
[7] R. J. Chandler, S. Gibson,V. Karkare, S. Farshchi, D. Markovic and J. W. Judy, "A system-level view of optimizing high-channel-count wireless biosignal telemetry," in *Proc. Annu. Int. Conf. IEEE EMBS*, 2009, pp. 5525–5530.
[8] S. Ray, Y. Jin, and A. Raychowdhury, "The changing computing paradigm with internet of things: A tutorial introduction," *IEEE Des. Test Comput.*, vol. 33, no. 2, pp. 76–96, Apr. 2016.
[9] F. Palermo, "Internet of things done wrong stifles innovation," [Online]. Available: http://www.informationweek.com/strategic-cio/executive-insights-and-innovation/internet-of-things-done-wrong-stifles-innovation/a/d-id/1279157?page_number=1, Accessed Apr. 21, 2016.
[10] M. weiser, "The computer for the 21st century," *Sci. Amer.*, vol. 265, no. 3, p. 2014, 1991.
[11] R. Raji, "Smart networks for control," *IEEE Spectr.*, vol. 31, no. 6, pp. 49–55, Jun. 1994.
[12] D. Kyriazis, T. Varvarigou, A. Rossi, D. White, and J. Cooper, "Sustainable smart city iot applications: Heat and electricity management and Eco-conscious cruise control for public transportation," in *Proc. IEEE Int. Symp. Workshops World Wireless, Mobile Multimedia Netw.*, 2013, pp. 1–5.
[13] S. Li, H. Wong, T. Xu, and G. Zhou, "Application study on internet of things in environment protection field," *Lecture Notes Electr. Eng.*, vol. 133, pp. 99–106, 2011.
[14] S. Ray and Y. Jin, "Security policy enforcement in modern SoC designs," in *Proc. 34th Int. Conf. Comput.-Aided Des.*, 2015, pp. 435–530.
[15] A. Basak, S. Bhunia, and S. Ray, "A flexible architecture for systematic implementation of SoC security policies," in *Proc. 34th Int. Conf. Comput.-Aided Des.*, 2015, pp. 536–543.
[16] S. Ray, J. Yang, A. Basak, and S. Bhunia, "Correctness and security at Odds: Post-silicon validation of modern SoC designs," in *Proc. 52nd Int. ACM/EDAC/IEEE Des. Autom. Conf.*, 2015, pp. 1–6.
[17] S. Narasimhan, H. J. Chiel, and S. Bhunia, "Ultra-low-power and robust digital-signal-processing hardware for implantable neural interface microsystems," *IEEE Trans. Biomed. Circuits Syst.*, vol. 5, no. 2, pp. 169–178, Apr. 2011.
[18] S. Narasimhan, X. Wang, and S. Bhunia, "Implantable electronics: Emerging design issues and an ultra light-weight security solution," in *Proc. IEEE Annu. Int. Conf. Eng. Med. Biol. Soc.*, 2010, pp. 6425–6428.
[19] S. Paul and S. Bhunia, "Reconfigurable computing using content addressable memory for improved performance and resource usage," in *Proc. 45th Annu. Des. Autom. Conf.* , 2008, pp. 786–791.
[20] L.-y. Chiou, S. Bhunia, and K. Roy, "Synthesis of application-specific highly efficient multi-mode cores for embedded systems," *ACM Trans. Embedded Comput. Syst.*, vol. 4, no. 1, pp. 168–188, 2005.

Sandip Ray (M'12–SM'13) received the PhD degree from the University of Texas, Austin. He is a research scientist in the Strategic CAD Labs, Intel Corporation. His research focuses on developing trustworthy embedded, mobile, and IoT systems through a synergy of architecture, synthesis, and validation techniques. He is a senior member of the IEEE and professional member of the ACM.

Jongsun Park (M'05–SM'13) is currently an associate professor in the School of Electrical and Computer Engineering, Korea University, Seoul, Korea. His research interests focus on variation-tolerant, low-power, and high-performance VLSI architectures and circuit designs for digital signal processing and digital communications. He is a senior member of the IEEE.

Swarup Bhunia (S'00–M'05–SM'09) received the BE (Hons.) degree from Jadavpur University, Kolkata, MTech degree from the Indian Institute of Technology, Kharagpur, and the PhD degree from Purdue University, IN. He is currently a professor at University of Florida. Earlier, he was appointed as the T. and A. Schroeder associate professor of electrical engineering and computer science at Case Western Reserve University. He has more than 10 years of research and development experience with more than 200 publications in peer-reviewed journals and premier conferences. His research interests include hardware security and trust, adaptive nanocomputing, and novel test methodologies. He is a senior member of the IEEE.