Editorial: Cyber Security, IoT, Block Chains—Risks and Opportunities

A DNS hijacking attack this week in India defaced the websites of some of the major academic institutes in the country, even though the attack did not touch the web servers inside any of the institutes. The postmortem analysis is yet to be published, but the guess is that the ac.in domain name server was hijacked, and all domain records were changed to point to a server where subversive content was being displayed. During the summer of 2016, it seems that the ATM machines from a specific make running on Windows XP were infected by malware and about 3.2 million debit cards from various Indian banks were compromised. The recent election in several Indian states and the surprising results led to a controversy on the security of the electronic voting machines in India. A banking access protocol known as unified protocol interface (UPI) was hacked to siphon off funds from an Indian bank in April. There has been a massive data breach in an Indian State's storage of universal identification data for pensioners.

The US presidential election cycle was entangled with cyber breaches of information systems and e-mail accounts of important players and the controversy is still raging. In the meantime, the IoT botnet Mirai created a deluge of domain name translation requests leading to a denial of service attack on the top-level domain name servers maintained by Dyn. The bitcoin block size debate is raging in the cryptocurrency circles, and a hard fork in the bitcoin seems to be imminent. Ethereum-based block chain is gaining popularity not for crypto currency but for many interesting applications such as tracking transactions of various kind, especially the access to sensitive data such as health data in the UK.

Yesterday, there was a news that attracted attention of many—a nongovernmental organization that serves mid-day meals to underprivileged children is now tracking the serving of meals using the IoT and blockchain with the help of Accenture Lab. This surely qualifies as a great achievement of embedded systems, crypto, and artificial intelligence technology because instead of making money from technology, they are using technology for a social cause, and improve the quality of service to the underprivileged. This, in my view, should be hailed and followed. Technology is often used in the service of the society as technology improves our lives, livelihood, and our abilities to be more productive. But harnessing the latest trends in technology for humanitarian cause provides us with hope for the future among the grim pictures of we get every day with the myriads of stories about cyber-attacks, cyber-crime, weaponization of technology, and the use of science and technology for making money.

Relevance of IoT in the field of embedded systems is quite self-evident. Most IoT devices are embedded devices, often with real-time applications, and networking among them. However, blockchain might seem a rather different type of technology. Even though in the bitcoin world the ASIC-based hardware for mining blocks could be seen as example of high-performance embedded systems, that is not what I see as the relevance of blockchain in the field of embedded systems. What makes blockchains attractive in the domain of IoT and networked embedded systems is that it allows one to provide public key infrastructure without a centralized authority like a digital certificate issuer. It also allows one to keep track of important activities within the system, especially those associated with highly privileged user accounts in an immutable and non-repudiable form. One of the properties of a malware running havoc in a networked

1539-9087/2017/07-ART62
DOI: http://dx.doi.org/10.1145/3087913

system is that they usually change the log files to remove their own footprints. If the logging is committed to a block chain, it will be rather difficult to erase the footprints of the attacker—or so it seems.

A recent meeting with a technology investor in India revealed that a large number of engineering teams across India are leveraging IoT and machine learning technology to develop innovative solutions to various problems faced by a country like India. For example, low-cost health care, low-cost home energy management, and the health management of infrastructure seem to be popular choices for the start-up founders, and there is a variety of approaches and problem domains. Some of these have immense opportunity not just from a business perspective but also in making an impact to a society that requires low-cost technology solution in health care, in saving energy bills, or saving the aging infrastructure.

Therefore, my conclusion is that while the cyber security attacks, and possibly dooms day scenario such as Cyber 9/12 makes us grim and wary of the future—there are opportunities abound in using technology for a better society. The only caveat is that we need to make them resilient to cyber-attacks, and innovate techniques to survive in the face of untrustworthy environment. So, we have a lot to work on in the coming years.

This issue of *ACM Transactions on Embedded Computing Systems* is particularly interesting because we have three special issues embedded here—one on embedded systems and IoT, one on secure and fault-tolerant embedded computing, and another on embedded designs for extremely big data in large-scale devices. In the regular article section, we have a variety of topics covered—energy-efficient sensor networks, authentication in controller area networks, fault-tolerant aperiodic scheduling, breast cancer detection with accelerator coprocessors, binary translation, storage systems, solar-powered sensor networks, and so on. The journal has now truly become an exhibit for the diversity of topics that comprises the embedded computing field today.

One piece of good news—we are going to become bi-monthly from Volume 17 onward, allowing us to publish issues more frequently, and more articles. We also are going to experiment with the journal integrated conference model with ESWEEK (Embedded Systems Week) conference papers. The papers selected for the four conferences in the ESWEEK will appear in an online special issue of this journal, and no conference proceedings will be published. This will address the problem of publication explosion in our field where each paper is published twice—once in a peer-reviewed conference and then in an extended form in a journal. This puts immense pressure on one of our precious resources—reviewers. We hope to succeed in this experiment to at least partially address this issue.

[1] https://newsroom.accenture.com/news/accenture-labs-and-akshaya-patra-use-disruptive-technologies-to-enhance-efficiency-in-mid-day-meal-program-for-school-children.htm.

Sandeep K. Shukla

Indian Institute of Technology Kanpur

April 28, 2017

Editor-in-Chief