

The Indian Banking Community Cloud

Lalit Sangavarapu, Shakti Mishra, Abraham Williams, and G.R. Gangadharan,
Institute for Development and Research in Banking Technology, Hyderabad, India

Community clouds offer services to support organizations with shared objectives and common security and privacy requirements. By providing cloud-based services exclusively to Indian banks, the Indian Banking Community Cloud (IBCC) aims to address the financial sector's growing demand for secure cloud-based services.

As technologies evolve, businesses no longer view IT as a complex and time-consuming aspect of the decision-making process. Gone are the days when businesses waited for IT personnel to provide the computing power and applications necessary to support decision making through data processing. With the advent of virtualization technologies, cloud computing has come a long way in a short time, making it easier to access and analyze volumes of data. In particular, cloud computing is having a significant impact on operations and IT department functions within the banking, financial services, and insurance (BFSI) sector, which relies heavily on IT for decision making and keeping track of business operations.¹

BFSI is a dynamic sector that continually adjusts to changing business, political, and socio-economic conditions. For BFSI operations dealing either with customers or internal operations, IT is both widespread and deeply rooted. This raises several challenges in relation to IT assets and infrastructure:

- Although their primary business is banking, banks must allocate a big chunk of their budgets each year to IT departments and services.
- With increasing complexity and demand for huge data storage, computing power, and security (both physical and logical), banks must continually provide IT infrastructure, including servers, networking and security devices,

network cabling, and electrical and cooling systems.

- Setting up such datacenters—with their demands related to electrical energy, environmental controls, safety and security, and maintenance and management—is a tedious process.
- Provisioning a new IT service in banks, whether customer facing or for internal purposes, is typically a long process.

At the Institute for Development and Research in Banking Technology (IDRBT)—an organization established by the Reserve Bank of India—we've developed a cloud-based approach for addressing these challenges. The Indian Banking Community Cloud (IBCC) initiative aims to help banks reduce costs and save resources while providing efficient and secure services.

Cloud Adoption and the BFSI Sector

Cloud computing has been a major focus of business organizations around the world. Cloud computing is an IT-servicing technology built on the idea of exploiting virtualization technology's shared resource pooling, as well as its scalability and elasticity. To provision new IT services rapidly and get them to market faster, BFSI sector organizations are increasingly looking to adopt cloud computing technology, which offers the following advantages:

- BFSI organizations could realize a considerable decrease in their total cost of ownership, as well as increased flexibility and agility, and relief from software licensing management.
- Organizations could consolidate several servers and applications into minimal physical hardware, thereby reducing costs for hardware maintenance, real estate, IT personnel, and so on.
- Beyond cost savings, the cloud would provide banks with opportunities to build customer-centric and active business models to grow their brands more efficiently.²

Despite such benefits, many BFSI institutions are hesitant to try external providers' cloud services because of

- security concerns,
- insufficient regulatory standards,

- problems with interoperability,
- ambiguous service features, and
- insufficient governance mechanisms.

Security is the primary concern; BFSI organizations fear abusive and nefarious usage, insecure APIs, data loss or leakages, and malicious insiders. The second major concern is lack of regulatory standards, including compliance with jurisdictional laws and regulations, and legal liability. Interoperability is also a concern, because it makes adopting and migrating applications and data to the cloud difficult. Challenges here include vendor lock-in, technology lock-in, and licensing-related issues. Another challenge is ambiguous service features, including those related to quality of service, reliability, availability, continuity, and support, as well as the lack of proper measurement and monitoring procedures and provider-sided service-level agreements (SLAs). Finally, the lack of governance mechanisms—including issues of ownership, accountability, business risks, and policy—is yet another major factor inhibiting cloud adoption.

Given this, BFSI organizations might prefer a private cloud setup, which would protect their existing infrastructure investments while also offering benefits from a cloud-like deployment. Although a private cloud setup is secure in nature, it might be infeasible for some BFSI organizations, especially small and medium sized ones. Also, the public cloud has many advantages, including lower service costs due to multitenancy and resource sharing, tiered service consumption, and lower up-front investments. However, the public cloud's security issue remains unsolved. Consequently, the IDRBT looked to develop a community cloud in which the cloud services targeted organizations with common objectives and security controls.

The Indian Banking Community Cloud

India's banking sector has 151 commercial banks, with an aggregate deposit of US\$1.1 trillion, as of March 2013, controlled and monitored by the Reserve Bank of India (http://en.wikipedia.org/wiki/Banking_in_India). In terms of quality of assets and capital adequacy, the Indian banking sector is considered to have clean, strong, and transparent balance sheets relative to other banks in comparable economies in its region.

To the best of our knowledge, the IBCC initiative is the first community cloud in the world for the banking sector. Its aim is to collaborate with various Indian banks to showcase optimized cost while maintaining desired levels of efficiency and security for banks.

Assessing Cloud Readiness

When a bank seeks to develop or port an application into the cloud, the IBCC team and the bank's technology team first must jointly assess the target application. This gives the IBCC team a broader view of the application's pros and cons and of how safe or risky the application is. Once the team has evaluated these conditions, it decides whether the application can be deployed in the cloud.

In particular, the IBCC team uses the Cloud Application Assessment tool to assess the application's software and hardware performance and estimate its security and risk levels. The tool helps identify the following:

- *Business value*: The tool examines the application's business-level priorities in terms of its business benefit (elasticity, flexibility, standardization, real estate, and so on); alternate device support (mobile devices); application criticality; availability requirements; and whether it is internally or externally facing.
- *Technology readiness*: The tool ensures that the application is ready at all levels, including the system and software architecture, data flow, software stack, virtualization level, and network requirements.
- *Operational risk readiness*: The tool performs vulnerability assessment and penetration testing for all applications being deployed, checking identity and management requirements, available interfaces, intrusion detection and prevention systems, firewall security, data sensitivity, hardening requirements, and the bank's information security guidelines.

Furthermore, the Cloud Application Assessment tool uses a scale of 1–10 for questions related to all three of these factors. Based on each question's established priority and the bank's responses, the tool provides a Kiviati diagram on cloud readiness. Once clients complete the assessment, the IBCC team evaluates the assessment using benchmark

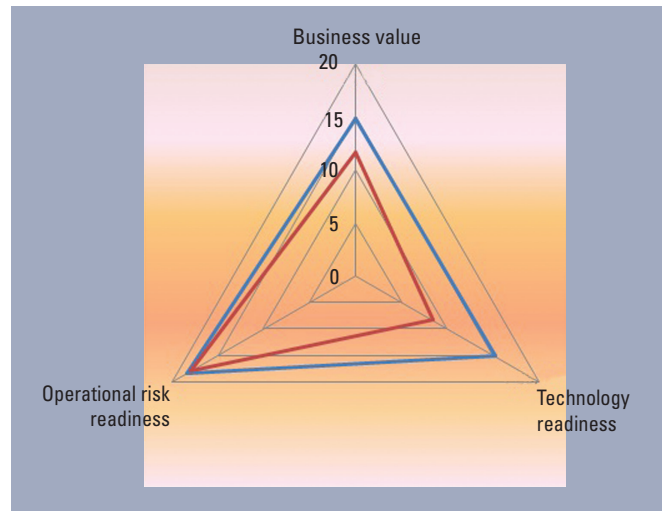


Figure 1. A sample estimation for Bank ABC's proposed application and the corresponding Kiviati diagram. The red lines represent the benchmark values (12, 8, and 18, for business, technology, and operational levels, respectively) and the blue lines represent the assessment values (15, 15, and 18).

values to see if the application meets the cloud environment's standards, which have been determined by cloud computing domain experts and banking professionals. The benchmark values show the average values required for an application to be suitable for hosting in a cloud environment.

As an example, say that Bank ABC submits estimation values for its application's business, technology, and operational levels of 15, 15, and 18, respectively, and that the related benchmark values are 12, 8, and 18, respectively. Figure 1 shows the resulting Kiviati diagram, which gives a clear comparison between the benchmark and application's assessment values.

As the Kiviati diagram shows, Bank ABC's application can be deployed in the cloud with no dilemma.

Architectural Layers

The IBCC is built on the Meghdoot stack (<http://cdaccloud.com/meghdoot>), which was adopted from the Eucalyptus Community Edition and is available as free open source software.³ To ensure both confidence in cloud services and a steady approach for cloud deployment, the IBCC team recommends moving less critical and internal-facing applications to the cloud. The IBCC currently supports Intel's x86-based architecture platform.

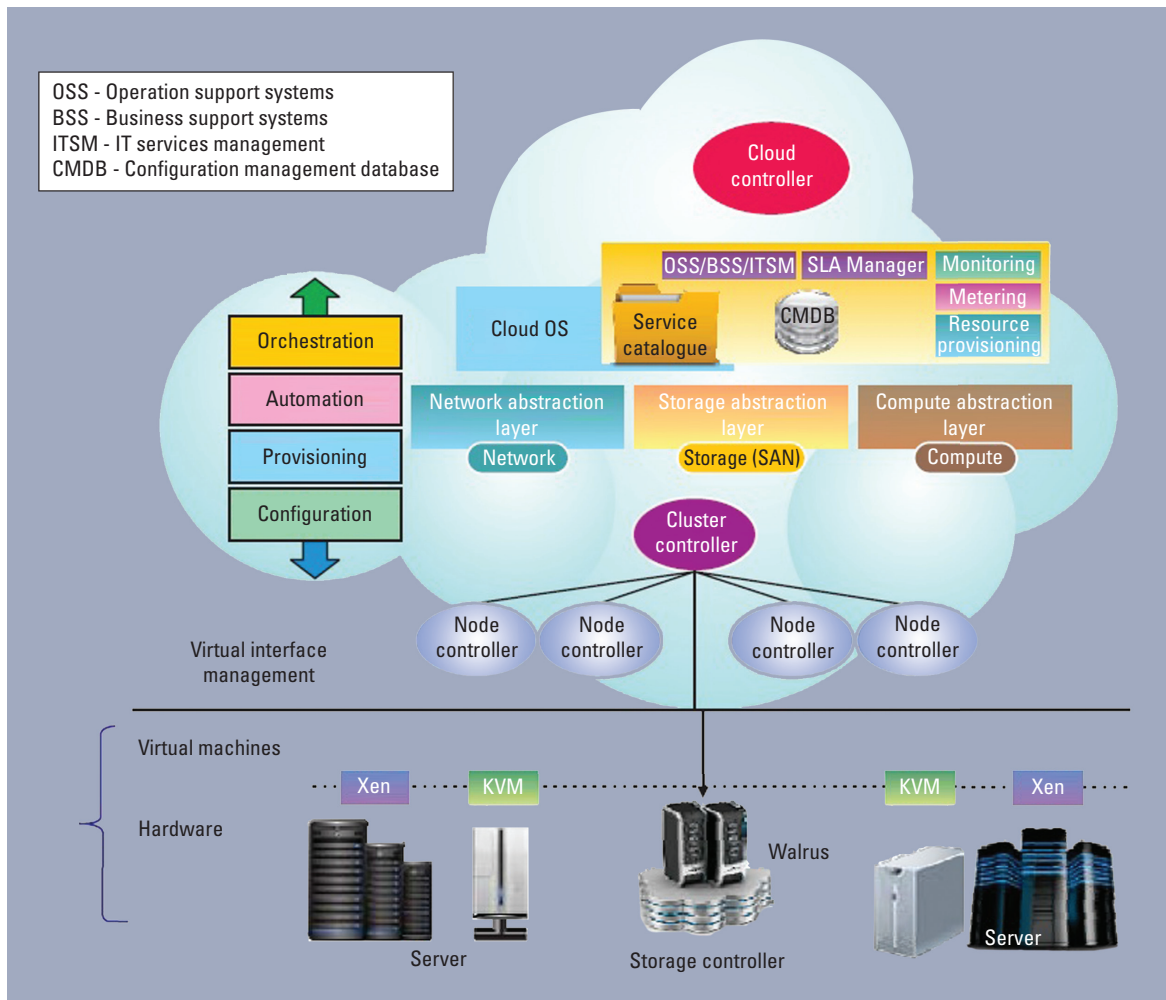


Figure 2. Indian Banking Community Cloud architecture. This initiative by the Institute for Development and Research in Banking Technology in Hyderabad, India provides cloud-based services exclusively for Indian banks.

Figure 2 shows the IBCC cloud architecture. The lowermost layer is the hardware infrastructure, which stores the data and applications. Above that physical infrastructure lie the virtual machines (VMs), while above those is the virtual interface management layer, which holds the Eucalyptus components (including the cloud, cluster, and storage controllers).⁴

As Figure 2 shows, the cloud software stack has many key components. The *cloud controller* is the entry-point into the cloud for administrators, developers, project managers, and end users. The cloud controller also interfaces between other components for information about resources, makes high-level scheduling decisions, and makes requests of the *cluster controller*.

The cluster controller is the interface to the management platform and exposes underlying

virtualized resources (servers, network, and storage). *Walrus* lets users store persistent data organized as buckets and objects. It provides a mechanism for storing and accessing VM images and user data. The cluster controller gathers information about a set of node controllers and schedules VM execution on specific node controllers. It also manages the VM networks. All node controllers associated with a single cluster controller are in the same subnet. The *storage controller* functions similarly to the Amazon Elastic Block Store and can interface with various storage systems. A node controller can execute on any machine that hosts VM instances; node controllers control VM activities, including the execution, inspection, and termination of VM instances. They're also the physical servers that host the VMs using hypervisors.

Figure 2's left side shows several layers, each with specific functionalities. *Provisioning* and *configuration layers* let cloud providers offer priority services to consumers in terms of VMs, data access, infrastructure resources, and so on. *Automation* and *orchestration layers* handle the automated arrangement and management of the service provider's services and dynamically attach the services to the consumers based on cloud service provider norms and consumer specifications.

The upper right of the cloud shows the operation support systems, business support systems, and IT service management, which are adopted to manage cloud computing's operational and business-related functionalities. IBCC services are managed through the Web-based Meghdoot service portal, which helps banks decide which types of services their applications can use. The *SLA manager* takes care of the SLAs between the service provider and the banks using the cloud services.

The *configuration management database* houses information about the various resources related to an organization's IT infrastructure, including data about managed resources, such as computers, application software, and process records. The Hyperic utility (www.hyperic.com) is built into IBCC and performs the *monitoring* and other logging functions, verifying each cloud resource's performance and functionalities to avoid failure events.⁵ The Meghdoot service portal also includes an interface to manage resources, including nodes, applications, and their cost. *Metering* ensures proper functioning of utilities, including a machine's disk space and network and memory usage.⁵ A refined metering plan lets cloud providers monitor actual resource usage by consumers and charge them accordingly. The accurate usage information provided by metering offers consumers a pay-per-use model. Based on the average VM size, utilization rate, and available projections, the pricing for usage is calculated. The IBCC team has adopted a "cost plus margin" strategy⁶ for billing, and banks are charged on a monthly basis for their usage.

The IBCC uses the Multiprotocol Label Switching (MPLS) network cloud and leased lines with and without redundancy to connect bank datacenters and the IBCC. The *network abstraction*

layer is wrapped with Internet protocol security (IPSec), with required intrusion detection and prevention systems and firewalls in place. Also, each bank is in a separate VLAN environment and can use its existing active directory services for access and identity management. Banks using platform as a service (PaaS) or infrastructure as a service (IaaS) must set up their own applications. However, for some applications already available as software as a service (SaaS), banks need only provide access.

Data Recovery

The IBCC has built-in images provided by the cloud software stack, and VM administrators can also create, upload, and register images. However, only the cloud administrator user can upload and register kernel or RAM disks. The IBCC team recommends that users bundle images with the installed VM applications for faster recovery procedures. Banks can bundle the images on their own or ask the service provider to do it whenever an application update occurs. For every VM change—including to the database software, operating system, antivirus software, or application (in the form of a patch or other change)—the image must be bundled to ensure that application images are available for scalability. The running instance can be bundled as a new image. The bundled image is relaunched as a new instance with all the applications running.

It's possible to achieve a well-planned disaster recovery that retrieves lost data smoothly and easily without any unpredictable failures. In the IBCC, all VMs are backed-up daily; each day's snapshot is kept for seven days before the space is recycled. The IBCC supports a second availability zone (far site) that will host applications if a bank wants high availability for its applications.⁷ This zone runs asynchronous site-to-site replication between the storage devices.

Operation Guidelines and Roles

For day-to-day operations, the IBCC has operating guidelines and a contract with the banks. The operating guidelines provide workflow details for implementation, incident reporting, escalation mechanisms, SLAs, the exit process, and metering aspects. To ensure SLA governance and adherence, the IBCC team forms a working group with the

banks. Some of the IBCC team's internal roles include

- *program managers*, who build use cases, interact with banks, and lay the roadmap for managing the IBCC;
- *cloud architects*, who do research and convert the roadmap to a technology architecture;
- *cloud administrators*, who provision the VM and enhance IBCC features;
- *cloud support staff*, who monitor and ensure the availability of the hardware, network, and VM; and
- *cloud testers*, who build regression suites and validate deployment correctness.

These roles provide support for banks deployed in the IBCC environment and help build future requirements for the cloud environment.

Services Offered

The IBCC provides IaaS, PaaS, and SaaS for banks in India. Among the services IBCC offers to banks, the following three are the most popular.

Technology risk assessment. The Technology Risk Assessment Modeling System (TRAMS) is an application deployed in SaaS mode in the IBCC. TRAMS provides an interface for application and asset risk assessment. The system comes with a prefilled questionnaire based on several standards, including ISO 27001; the Payment Card Industry Data Security Standard (PCI DSS); recommendations from the Reserve Bank of India's Working Group on Information Security, Electronic Banking, Technology Risk Management, and Cyber Frauds Committee;⁸ and Open Web Application Security Project (OWASP; www.owasp.org) guidelines for alternate banking channels (Internet, mobile, ATMs, and phone banking). The system also provides a trends chart, compliance report, and other risk-monitoring features.

Learning management. With the increase in bank branches across India and a younger workforce joining India's banking sector, banks realized the need for e-learning. Also, it's now crucial to make learning opportunities flexible and available at the learner's pace, which means banks must offer e-learning in an environment that is always accessible and scales in and out based on usage.

With the IBCC, some remote branches still run on a *very small aperture terminal* (VSAT) with very low bandwidth. Because banks use most of their bandwidth for transaction processing, deploying e-learning in a private network (LAN) creates bandwidth constraints. Having the IBCC host an e-learning solution has thus aided the banking industry here; the environment is available on the Internet for bankers and can scale its features based on usage demand. The environment is also secure for a bank's staff human resources data, which is a concern banks have if the data is in a public cloud.

Email. Regional Rural Banks (RRBs) in India are small banks that serve the daily needs of farmers and SMEs. Today, bank branches communicate using public email accounts—raising concerns about snooping—so with guidance from the government, RRBs are exploring secured means of email communication. As part of this, the IBCC team sets up a pilot project that provides 5,000 mailboxes for three regional rural banks in the IBCC environment; RRBs can use the mailboxes for a monthly fee based on usage.

Security Aspects

Security is of paramount importance in cloud computing, and the IBCC team is working to implement the best security practices. The IBCC team developed a cloud security framework based on the available guidelines from the US National Institute of Standards and Technology, PCI-DSS, the European Network and Information Security Agency, and the Cloud Security Alliance, and recommendations from chief information security officers in the Indian banking sector. This framework is used to implement IBCC security. Also, the IBCC gives banks the flexibility of performing audits with or without giving prior notice to the IBCC team. In addition, the IBCC environment will be audited by an independent, qualified auditor every six months, and the resulting security report will be shared with member banks.

The data at rest is encrypted and stored on the storage environment to ensure that even cloud administrators can't access or modify data. The data in motion is encrypted through the Internet Protocol Security (IPSec) and generic routing encryption (GRE) tunnel, as well as

Table 1. The Indian Banking Community Cloud’s security levels and controls.

Security level	Controls
Access to server room	Three levels of access control (biometric, PIN, and access card)
Hardware	Kept under lock and key in the access-controlled datacenter Password protected IP-based cloud machines access
Cloud stack	Virtual machine (VM) access through public key infrastructure Data encryption using Advanced Encryption Standard (AES) algorithm Firewall at cloud stack
Network	Internet Protocol Security (IPSec) and generic routing encryption (GRE) tunnel Network firewalls Intrusion detection and prevention systems VMs are in the bank’s designated VLAN; even cloud administrators can’t access them
Identity management	Strong user ID and password Application access requires single sign-on, Active Directory, and Lightweight Directory Access Protocol integration
Application	Certified by security experts
Database	Data encryption by AES 128-bit data encryption
Anti-virus	Updates and patches on VM Server-level anti-virus protection
Operating system security	Updates and patches on VM Updates and patches at cloud stack
Internet	Internet access and file download access on VM disabled by default
People	IBCC team members are aware of security requirements and have undergone background verification

by using a virtual LAN with a software switch available in the Meghdoot stack. Hypervisor’s zoning ensures segregation of access rights and privileges between hardware and the virtual environment. Finally, the IBCC manages the datacenter according to industry standards. Table 1 shows some of the security controls the IBCC is adopting.


Deployment Challenges

Deploying applications in the cloud can create challenges in two key areas:

- *Legacy code.* When applications contain legacy code, it can interrupt their execution in the cloud environment. Implementing legacy code in a cloud environment can give rise to several issues, including a lack of vendor support, documentation, and manpower to debug the code.
- *Fluctuating requirements.* For some applications, storage and physical resource requirements can rise or drop suddenly at particular times. Rendering resources at such peak times can be risky because justifying the heights of security and risk vulnerabilities, data storage capacities,

and extra resources allocation on demand remains unpredictable.

The IBCC team continues its effort to improve the cloud environment for banks in India.

The IBCC team is currently working on several areas. First, we’re working to provide SaaS for common banking-related applications—including analytics and anti-money laundering—and to provide interoperability across cloud software stacks. We’re also implementing vertical scaling to contend with the fact that most of the less-critical applications are deployed in a single server, so moving them to IBCC would help only if that single server could support increased computing resources at runtime on the same VM rather than creating another VM (vertical scaling). Finally, we’re supporting IBM P Series machines and other architectures in addition to X86 architecture, because India’s banking community uses these other architectures for critical applications and transaction-oriented applications. 

References

1. D. Benton and W. Negm, *Banking on the Cloud*. tech. report, Accenture, 2010.
2. E. Oliveros et al., "Monitoring and Metering in the Cloud," in *Achieving Real-Time in Distributed Computing: From Grids to Clouds*, IGI Global, 2011, p. 94–114.
3. D. Nurmi et al., "The Eucalyptus Open-source Cloud-computing System," *Proc. 9th IEEE Int'l Symp. Cluster Computing and the Grid*, 2009, pp. 124–131.
4. Y. Wadia, "The Eucalyptus OpenSource Private Cloud," *CloudbookJ.*, vol. 3, no. 1, 2012; www.cloudbook.net/resources/stories/the-eucalyptus-open-source-private-cloud.
5. S. Jain, *Managerial Economics*, Pearson Education, 2006.
6. G. Sattiraju, L. Mohan, and S. Mishra, "IDRBT Community Cloud for Indian Banks," *Proc. Int'l Conf. Advances in Computing, Communications, and Informatics (ICACCI)*, 2013, pp. 1634–1639.
7. A. Garg, *Cloud Computing for the Financial Services Industry*, tech. report, Sapient, 2011.
8. Working Group on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds Committee, *Report and Recommendations*, Reserve Bank of India, Jan. 2011; <http://rbidocs.rbi.org.in/rdocs/PublicationReport/Pdfs/WREB210111.pdf>.

Lalit Sangavarapu is a senior technology manager in the Strategic Business Unit at the Institute for Development and Research in Banking Technology (IDRBT) in Hyderabad.

His research interests include cloud computing, information security, and analytics. Sangavarapu has a Bachelor's in Technology from Jawaharlal Nehru Technological University, India, and he is pursuing his PhD in computer science at the International Institute of Information Technology, India. Contact him at slmohan@idrbt.ac.in.

Shakti Mishra is an assistant professor at the Institute for Development and Research in Banking Technology (IDRBT) in Hyderabad. Her research interests include distributed systems and formal methods. Mishra has a PhD from the National Institute of Technology, Allahabad, India. Contact her at mishra.mahi@gmail.com.

Abraham Williams is a technology manager at the Institute for Development and Research in Banking Technology (IDRBT) in Hyderabad, India. His research interests include cloud computing, networks, and security. Williams has an MS in information systems from Osmania University, India. Contact him at akwilliams@idrbt.ac.in.

G.R. Gangadharan is an assistant professor at the Institute for Development and Research in Banking Technology (IDRBT) in Hyderabad. His research interests include Internet technologies, green IT, and the interface between technological and business perspectives. Gangadharan has a PhD in information and communication technology from the University of Trento, Italy, and the European University Association. He is a Senior Member of IEEE and ACM. Contact him at geeyaar@gmail.com.

IEEE computer society

PURPOSE: The IEEE Computer Society is the world's largest association of computing professionals and is the leading provider of technical information in the field.

MEMBERSHIP: Members receive the monthly magazine *Computer*, discounts, and opportunities to serve (all activities are led by volunteer members). Membership is open to all IEEE members, affiliate society members, and others interested in the computer field.

COMPUTER SOCIETY WEBSITE: www.computer.org

Next Board Meeting: 16–17 November 2014, New Brunswick, NJ, USA

EXECUTIVE COMMITTEE

President: Dejan S. Milojicic

President-Elect: Thomas M. Conte; **Past President:** David Alan Grier; **Secretary:** David S. Ebert; **Treasurer:** Charlene ("Chuck") J. Walrad; **VP, Educational Activities:** Phillip Laplante; **VP, Member & Geographic Activities:** Elizabeth L. Burd; **VP, Publications:** Jean-Luc Gaudiot; **VP, Professional Activities:** Donald F. Shafer; **VP, Standards Activities:** James W. Moore; **VP, Technical & Conference Activities:** Cecilia Metra; **2014 IEEE Director & Delegate Division VIII:** Roger U. Fujii; **2014 IEEE Director & Delegate Division V:** Susan K. (Kathy) Land; **2014 IEEE Director-Elect & Delegate Division VIII:** John W. Walz

BOARD OF GOVERNORS

Term Expiring 2014: Jose Ignacio Castillo Velazquez, David S. Ebert, Hakan Erdogmus, Gargi Keeni, Fabrizio Lombardi, Hironori Kasahara, Arnold N. Pears
Term Expiring 2015: Ann DeMarle, Cecilia Metra, Nita Patel, Diomidis Spinellis, Phillip Laplante, Jean-Luc Gaudiot, Stefano Zanero
Term Expiring 2016: David A. Bader, Pierre Bourque, Dennis Frailey, Jill I. Gostin, Atsuhiko Goto, Rob Reilly, Christina M. Schober

EXECUTIVE STAFF

Executive Director: Angela R. Burgess; **Associate Executive Director & Director, Governance:** Anne Marie Kelly; **Director, Finance & Accounting:** John Miller; **Director, Information Technology & Services:** Ray Kahn; **Director, Membership Development:** Eric Berkowitz; **Director, Products & Services:** Evan Butterfield; **Director, Sales & Marketing:** Chris Jensen

COMPUTER SOCIETY OFFICES

Washington, D.C.: 2001 L St., Ste. 700, Washington, D.C. 20036-4928

Phone: +1 202 371 0101 • **Fax:** +1 202 728 9614 • **Email:** hq.ofc@computer.org

Los Alamitos: 10662 Los Vaqueros Circle, Los Alamitos, CA 90720

Phone: +1 714 821 8380 • **Email:** help@computer.org

MEMBERSHIP & PUBLICATION ORDERS

Phone: +1 800 272 6657 • **Fax:** +1 714 821 4641 • **Email:** help@computer.org

Asia/Pacific: Watanabe Building, 1-4-2 Minami-Aoyama, Minato-ku, Tokyo 107-0062, Japan • **Phone:** +81 3 3408 3118 • **Fax:** +81 3 3408 3553 • **Email:** tokyo.ofc@computer.org

IEEE BOARD OF DIRECTORS

President: J. Roberto de Marca; **President-Elect:** Howard E. Michel; **Past President:** Peter W. Staeker; **Secretary:** Marko Delimar; **Treasurer:** John T. Barr; **Director & President, IEEE-USA:** Gary L. Blank; **Director & President, Standards Association:** Karen Bartleson; **Director & VP, Educational Activities:** Saurabh Sinha; **Director & VP, Membership and Geographic Activities:** Ralph M. Ford; **Director & VP, Publication Services and Products:** Gianluca Setti; **Director & VP, Technical Activities:** Jacek M. Zurada; **Director & Delegate Division V:** Susan K. (Kathy) Land; **Director & Delegate Division VIII:** Roger U. Fujii

revised 23 May 2014

