Mils-Cloud: A Sensor-Cloud-Based Architecture for the Integration of Military Tri-Services Operations and Decision Making

Sudip Misra, Anuj Singh, Subarna Chatterjee, and Mohammad S. Obaidat, *Fellow, IEEE*

***Abstract*—Spatially distributed sensor nodes in wireless sensor networks (WSNs) can be used to monitor large unmanned areas. However, there are many limitations to WSNs, and the influence and accessibility of the sensors in these networks are limited to localized areas. Another popular technology today is cloud computing (CC). CC can provide a potent and scalable processing and storage infrastructure that can be used to perform the analysis of online as well as offline data streams provided by the sensors. It is possible to virtualize the sensor networks to provide these networks as a utility service. In this paper, we propose "Mils-Cloud," which is a sensor-cloud architecture utilizing this infrastructure for developing architecture for the integration of military tri-services in a battlefield scenario. We propose a hierarchical architecture of sensor-cloud with users having different levels of priority. The results show that reserving about 20%–25% of resources actually boosts the performance of the system for priority users without compromising the availability for normal users.**

***Index Terms*—Cloud architecture systems, cloud computing (CC) systems, military communications, sensor-cloud.**

I. Introduction

CURRENTLY, the defense forces worldwide are utilizing the advancements of technology in a very versatile manner. Defense forces generally operate in demanding and dynamically changing environments. In a battlefield scenario, it is a challenging task for defense forces to achieve real-time situational awareness. The applications of wireless sensor networks (WSNs) for enhancing functionalities such as monitoring remote unmanned areas are well known. However, the influence of WSNs is limited to a small area, and the benefits can be gained by a limited few. With the advent of the cloud computing (CC) paradigm, it is possible to integrate CC with WSNs [1]. Sensor-cloud can be utilized to achieve a higher level of command and control by providing utility services for defense forces on sensor-cloud architecture. In this paper, we propose "Mils-Cloud" architecture to ensure the highest level of coordination in three military services and integrate them through a sensor-cloud.

The objective is to design a *sensor-cloud* architecture for the integration of tri-services, i.e., a system that can be used to bring all the services of armed forces, viz., army, navy, and air force, on a common platform for better command and control, improve the real-time situational awareness of the battlefield, and enhance the ability of resource sharing. Keeping the specific military objectives in mind, a sensor-cloud-based system is best suited for it because sensor networks are widely used in the military domain, and their integration with CC enhances their utilization and helps to overcome their inherent shortcomings. Currently, all three services of the defense services, viz., army, navy, and air force, have to coordinate with each other during operations; however, all three services are independent of each other in terms of their resources, communication, and networks. The commanders at various levels of all of these three services can be aware of the real-time situation and can take a stock of things for planning and coordination in a better way if they are on the same platform, which "Mils-Cloud" aims to provide.

There have been some projects related to the use of CC technology [2] in the military by a few countries. The researchers at the Communications Electronics Research, Development and Engineering Center (CERDEC) of the U.S. Army are working on a cloud-based command and control platform. This platform enables soldiers to access crucial command control and intelligence services with a wide variety of military computers of variable link capacities located anywhere in the battlefield. Whereas, traditionally, defense forces operate using systems designed for using proprietary protocols and networks that lead to the isolation of these systems from one another [3]. Another initiative is being carried out by the U.S. Department of Defense (DoD) called Rapid Access Computing Environment (RACE), which is a private cloud providing Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) for DoD and is predominantly used for development and testing [4]. The benefits of CC is to decrease the total cost of ownership and, at the same time, provide cost-effective computing. CC provides an on-demand highly scalable storage and processing power to provide utility computing. There are three main classes of services provided through a CC environment, namely, IaaS, PaaS, and Software as a Service (SaaS) [2]. Keeping the features of CC and WSNs in mind, we can realize the benefits of sensor-cloud [5] in the military context [6]. The benefits that can be gained using

Manuscript received November 14, 2013; revised January 28, 2014; accepted March 26, 2014. Date of publication May 6, 2014; date of current version May 30, 2016.

S. Misra, A. Singh, and S. Chatterjee are with the School of Information Technology, Indian Institute of Technology Kharagpur, Kharagpur 721302, India (e-mail: smisra@sit.iitkgp.ernet.in; anujsingh@sit.iitkgp.ernet.in; subarna@sit.iitkgp.ernet.in).

M. S. Obaidat is with the Department of Computer Science and Software Engineering, Monmouth University, West Long Branch, NJ 07764-1898 USA (e-mail: obaidat@monmouth.edu).

Digital Object Identifier 10.1109/JSYST.2014.2316013

sensor-cloud platforms in a military environment are elaborated as follows.

1) *Real-time situational awareness*. Using this paradigm of sensor-cloud effectively, a service can be generated to achieve real-time situational awareness. For instance, the commanders at the highest level can gain information of the operating conditions, threats, and deployment at any instance.
2) *Higher level of cooperation*. There is always a requirement of high level of coordination and control during military operations. When all the forces, i.e., army, navy, or air force, are operational on one common platform, they can achieve higher coordination. Hence, the objective of tri-service integration can be achieved.
3) *Location independence*. Users can access information and undertake certain tasks without being dependent on a particular location, thereby providing flexibility and mobility.
4) *Information security*. Security can be enhanced by reducing the number of nodes having sensitive information by consolidating data on cloud storage, which is easier to handle.
5) *IT Infrastructure*. Sharing of resources and on-demand allocation as per requirement. For example, the same set of sensor nodes can be used by different users for different services.
6) *Accessibility*. Accessing sensor data over the cloud to enable better decision making and dissemination of commands.
7) *Handling heterogeneous devices*. Machines/sensors may not use interoperable OS, or system configuration may not allow the system to interact. However, using sensor-cloud services, a SaaS can be provided to get them synchronized.

The rest of this paper is organized as follows: In Section II, we briefly elaborate related work on sensor-cloud. Section III describes the basic idea of the "Mils-Cloud" and the proposed architecture. In Section IV, we bring out how the details of this platform can be used for integrating the three services. Section V brings out the challenges to be overcome during implementation of the proposed approach. Section VI gives the simulation analysis for the management of resources in the sensor-cloud using our approach, and Section VII gives out the conclusion.

II. Related Work

In recent times, there has been a lot of research in the field of sensor-cloud and the possibility of amalgamating the CC with WSNs has been explored [1]. Our work focuses on the use of sensor-cloud for military purposes. There have been few works in the past by some countries using the CC platform for military purposes, which can be found on the World Wide Web [3] and [4]. CC as a utility [2] and sensor-cloud infrastructure have been researched [5], [6]. Sensor networks can be integrated through the World Wide Web using CC, and the sensor nodes and cloud will interact using a SOA [7]. The military intelligence fusion concept given in [8] can be applied to the data in cloud. A software infrastructure using CC and the GPS system of mobile phones has been proposed for acquiring data from mobile devices and analyzing it to provide real-time situational awareness for better traffic movement [9]. Research has been carried out to manage data provided by body sensor networks through CC-based infrastructure [10]. Work has been done toward efficient streaming of multimedia information from mobile devices [11], http live streaming [12], and mobile learning application [13]. Works related to multimedia/video streaming in a WSN have been carried out recently [14], [15]. Zhou and Wang [14] aim to reduce the waiting time along with the fairness, whereas in our work, we aim to reduce the waiting period of priority users while there can be a compromise for normal users. Another work [15] focuses on reduction in distortion in video streaming while, at the same time, achieving fairness. Both works develop scheduling schemes specific to video streaming with traditional WSNs. However, the requirement of Mils-Cloud is for real-time access to sensor data in sensor-cloud architecture, which is different from the aforementioned works. In [16] and [17], interactions of sensors with the Web are discussed. CloudSIM [18] provides a platform for simulation of cloud-based infrastructure, which can be used for research activities.

III. Mils-Cloud: Proposed Architecture

A sensor-cloud infrastructure aims at providing support to the decision-making process by improving situational awareness. Defense forces adopt a hierarchical command structure to manage their resources, men, and equipment. The hierarchical architecture used is a result of the top-down decomposition of tasks and division of labor approach. The same paradigm is followed in the solution for developing this architecture. We illustrate the solution by taking an example of hierarchical formation such as Company (Cy), Battalion (Bn), Brigade (Bg), and Division (Dv). The model can be further expanded to incorporate a Corps or any other higher formation that may be practically present. However, for the purpose of explaining Mils-Cloud, we are truncating the hierarchy up to the division level. Figs. 1 and 2 depict a typical hierarchical deployment scenario of an army. The deployment of navy and air force is analogous, but the scales of distances and dynamism in movements may vary. The infrastructure may be materialized in a hierarchical fashion, taking into consideration the requirement of specific military conditions. The various companies and sensors deployed, as shown in Figs. 1 and 2, interact with a cloud. The cloud in the military context is typically a private cloud considering the security issues.

The sensors interact with sensor controllers on the cloud as per their location of deployment, i.e., they are grouped to form as per their locations. The various functions of the different modules are as follows.

1) *Sensor Network Controller*. This component maintains location data of various companies and sensors operating in the forward edges and groups them. It collects data from the sensors continuously or as and when requested by cloud services. It is responsible for providing services for the underlying sensor resources, e.g., power management and security. It carries out processing of data by

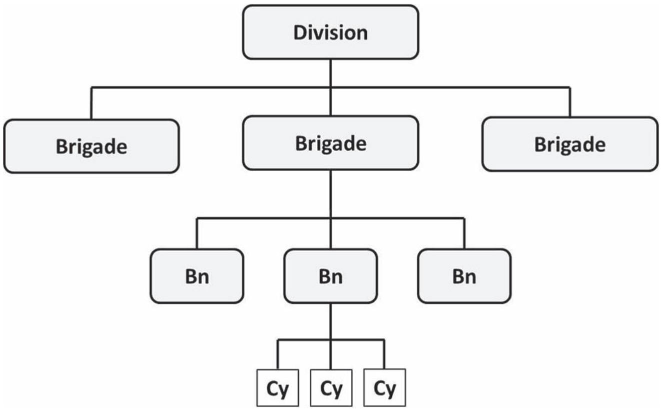

Fig. 1. Hierarchical model of deployment.

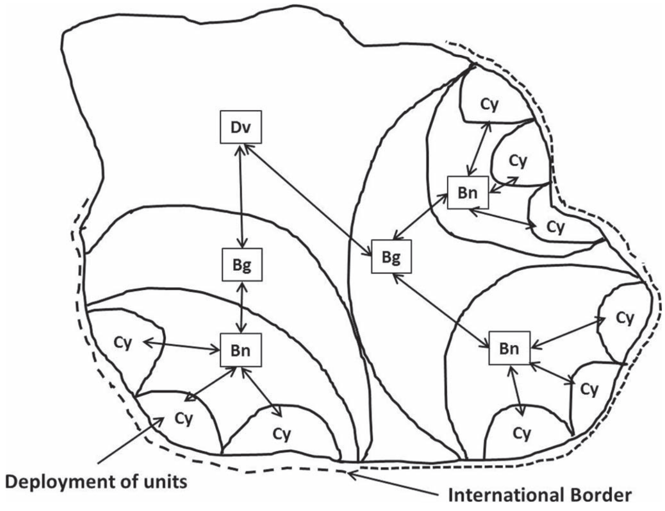

Fig. 2. Hierarchical model of deployment.

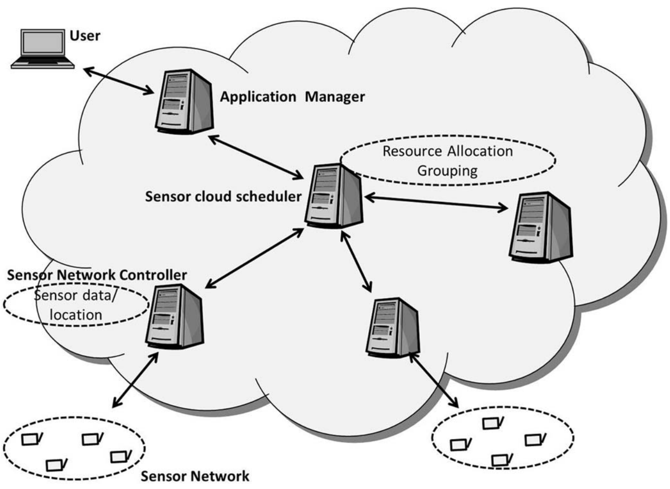

Fig. 3. Mils-Cloud architecture for military applications.

offloading the processing required to be done by sensors to cloud and increases the life expectancy of the sensors.

2) *Sensor Cloud Scheduler*. It maintains the grouping of various sensor controllers as per the location and further virtualization of resource under them. This component manages connectivity between sensor network controllers within the cloud. Resource allocation is done by this component on receipt of requests from an application. It also keeps a track of resources available and sharing of resources on cloud.
3) *Application Manager*. It forms the application interface of the military cloud. The battalion, brigade, and division interact with this module of cloud directly. On receipt of a request, it authenticates the credentials of a user, prioritizes the requests, and further sends to the sensor-cloud scheduler.

The workflow is explained in Fig. 3. The data from sensors are moved to the cloud through the sensor network controller. The data may be collected and stored for future use for analyzing the behavioral changes. Data can be kept in small files or in the form of XML messages with predefined tags.

The sensed data from the nodes have time stamps on them. The data are then processed for eliminating errors and format conversions. Once an application requires access to sensor data, the request is made through the application manager, which checks the credentials of the user so as to ascertain its privileges. The request is then prioritized on the basis of two criteria, namely, *urgency* and *confidentiality*. These two criteria are also associated with the users as their privileges. For example, the highest degree of confidentiality and urgency are associated with users at a higher level in the hierarchy such as commanders of Division. This is to implement a hierarchical model on the cloud at the application manager. Then, the application manager forwards the request to the sensor-cloud scheduler. The sensor-cloud scheduler analyzes the request and schedules it to a sensor network controller on the basis of location groups. If the scheduler finds a sensor network controller overloaded because of many queries from the same area, it virtualizes some sensor groups on another sensor network controller that is not utilized, thereby providing scalability of processing power in case of peaks. There can be many defense services that can be provided on this sensor-cloud architecture, e.g., a tool for implementing command and control, troop movement monitoring, causality evacuation and follow-up, pulling up logistic support as per requirement to maintain optimum stocking in forward areas, analyzing the stored sensor data, and help drawing inferences to enhance decision making.

The existing network topology can be modeled as a tree in the existing system, where the sensors are the leaves, and the formation at the highest level is the root. Let $D = \{D_1, D_2, \ldots, D_\alpha\}$, $B = \{B_1, B_2, \ldots, B_\beta\}$, $Bn = \{Bn_1, Bn_2, \ldots, Bn_\gamma\}$, and $C = \{C_1, C_2, \ldots, C_n\}$ represent the Dv, Bg, Bn, and Cy in the system, respectively, where $n > \gamma > \beta > \alpha$. We assume L to be the universal set of actors of the system, where $L = D \cup B \cup Bn \cup C$, and $l_i = level(L)$, $l_i \in L$. We model traffic load management and communication delay as the two parameters to establish the relevance of the proposed "Mils-Cloud."

A. *Traffic Load Management*

First, we model bandwidth utilization in the existing system at various levels. The lowest entity at level 1 is the company (Cy). Considering that sensor data have been acquired at this level, the flow of data is only upward. Hence, the traffic load T_c for Cy is modeled as

$$T_c = K \times l_i \times P \tag{1}$$

where l_i is the level of the querying entity, and P is the size of the packet. In this case, $K = 1$ because Cy being at level 1, there would only be response message being sent to the higher level. For modeling a Battalion (Bn), which is at level 2, there will be a broadcast of the query packet (P) downward to level 1, i.e., Cy. There are N entities at a level below the current mentioned level. It must be noted that, typically, in a military scenario, the value of $N = 3$. However, it may vary as per the demand of the situation. Therefore, for a Bn, i.e., level 2, the total traffic load T_{bn} is modeled as

$$T_{bn} = K \times N \times P \tag{2}$$

where K is the number of requests and responses in the system, i.e., for a request and response $K = 2$. It is assumed that there are three companies under a battalion. Focusing on the brigade level, it is assumed to have three battalions under it, and each battalion has three companies under it. Hence, in this case, the traffic load T_b becomes

$$T_b = K \times [N + N^2] \times P. \tag{3}$$

Similarly, for a division, which has three brigades under it, with each brigade having three Battalions and each battalion having three companies under it, we can derive the traffic load T_d as

$$T_d = K \times [N + N^2 + N^3] \times P. \tag{4}$$

This inference can be drawn by considering the Division to be at level 4. Similarly, there, we can work out for the higher formations, such as Corps and Command, in one service and, further, the highest level below, which are army, navy, and air force. Hence, the total traffic that will be broadcast in the system is

$$T_{Tot} = K \times [N + N^2 + \cdots + N^{l_i - 1}] \times P \tag{5}$$

where T_{Tot} is the total traffic on the system with query being generated at level l_i. Further, generalizing the model and keeping the number of entities as N under a particular level, we get

$$\begin{aligned} T_{Tot} &= K \times [N + N^2 + \cdots + N^{l_i - 1}] \times P \\ &= K \times \sum_{i=1}^{l_i - 1} N^i \times P \\ &= K \times N \frac{N^{l_i - 1} - 1}{N - 1} \times P. \end{aligned}$$

Therefore, T_{Tot} represents the total traffic on the existing system for broadcasting a query by a user at level l_i. However, if we analyze the traffic in "Mils-Cloud," we need to send the request to the application manager from where we can get data from the sensor-cloud infrastructure. We assume that the application manager is colocated with one of the entities in a hierarchy and that one entity needs to broadcast the request packet to the nearest application manager. Thereafter, data are extracted from the sensor-cloud infrastructure and furnished to the user. Hence, the request is broadcast to N neighboring entities until it reaches the application manager. Here, the equation becomes

$$T_{Tot} = K \times N \frac{N^{l_{diff}} - 1}{N - 1} \times P \tag{6}$$

where l_{diff} is the difference between the levels of the user and the level where the application manager is colocated. For example, if the application manger is located at the Bg level and a request is from the Dv level, the value of $l = 4$ in the conventional system is now brought down to $l_{diff} = 1$ with the help of "Mils-Cloud," and the rest of the links are free of any data traffic by this request, thereby reducing the data load on the system drastically.

B. Communication Delay

We analyze the effect of "Mils-Cloud" on communication delay. For simplicity, we denote the multiple-hop wireless communication time between two consecutive levels as a constant denoted by e. The logic of taking constant time is that formations at various levels are generally deployed in a homogeneous fashion and covering approximately similar areas at every level. Now, in a conventional system, if a user at a particular level l_i wants to know the requested sensor data from a particular location, then the units of delay, i.e., D, for that request is given by

$$D = K \times l_i \times e \tag{7}$$

where K is the number of requests and responses propagating in the system. It can be seen that the delay increases with the increase in level. Further, if we need to access sensor data from n locations, we need to traverse the entire link n times

$$D_{Tot} = \sum_{1}^{n} K \times l_i \times e. \tag{8}$$

However, in our proposed architecture of "Mils-Cloud," this delay can be reduced to a great extent by introducing the sensor-cloud infrastructure. The users, i.e., Division, Brigade, Battalion, and Company, can directly link to the cloud through the application manager and query for sensed data of multiple locations by a single request. The application manager will initiate the process of fetching the sensor data for the user request. Therefore, we achieve a delay that is independent of levels. In this scenario, the delay is calculated as the sum of delays to reach the *application manager*, sensor data to reach the *sensor network controller*, and the communication delay within the cloud. We assume that the application manager is colocated at one of the levels l. Then, the delay between the requesting level and the level of the application manager gives this part of delay l_{diff}. The delay within the cloud is taken to be a constant C_c, one time delay for sensor data to reach the sensor network controller. Therefore, the total delay units in "Mils-Cloud" is calculated as

$$D_c = K \times l_{diff} \times e + C_c. \tag{9}$$

We consider a scenario in which a division wants the sensed data from three different company locations. In Fig. 2, the time delay in units will be $8e$, considering the Dv at level 4, and for three locations, it amounts to $3 \times 8e$ i.e., $24e$. Whereas, in "Mils-Cloud," if we consider an application manager to be colocated at the Bg level and a user request arrives from the Dv level, the total delay in units is $2e + C_c$, $C_c < e$. Therefore, we get a total delay far lesser in "Mils-Cloud," as compared with the conventional system. The above model can be used for higher formations above division up to the apex level of army, navy, and air force.

IV. Tri-Services Cooperation

One major task that can be materialized by using a sensor-cloud is achieving a faster and more efficient way to achieve coordination at the highest levels. Traditionally, various command and control infrastructures of the military are designed to work on proprietary protocols and dedicated networks, which make it difficult to share information with different levels of hierarchy. Moreover, cooperation among different agencies, such as the army, navy, and air force, and other research and development organizations is difficult to achieve. However, by the use of a private cloud, we look for furtherance of this aim for cooperation at such high levels. In today's network-centric information warfare, the biggest challenge is to get own information and that of the enemy before the rival can do so. The three services (viz., army, navy, and air force) can specially work in coordination with each other during a conflict, and they require a very high degree of coordination to accomplish a mission. The sensor-cloud architecture proposed in this paper can be utilized to build a common platform where all the three services operate as a close-knit unit. We can virtualize three different parallel domains in the proposed architecture for military sensor-cloud, i.e., one for each of the three services. All three services operating on one private cloud enhance the resource-sharing capability, thereby adding flexibility and scalability to react to any adverse scenario. The three services can interact through an interservice communication module employed in the cloud, thereby making it possible for the three services to interact on the same platform for faster and real-time coordination. The layered platform for the sensor cloud architecture is shown in Fig. 4. The lowermost layer is the physical hardware, which includes all the resources on the cloud such as the CPU, memory, storage, sensors, and networking components. Directly over the physical hardware layer is the virtualization layer, which is responsible for visualizing the sensors, CPU, and memory. There are three verticals for the army, navy, and air force, which work on this platform. The three verticals can be further divided into operations, logistics, and administrative parts, to further improve the efficiency of infrastructure by streamlining the priorities. A number of different applications run on all the three verticals to manage their specific requirements. The concept of priority resolver and intercommunication module has been incorporated in the Mils-Cloud due to the existence of the three verticals. A subscription manger is used to identify the rights and privileges associated with a user. The rights and privileges of various users may vary as per the rank structure. Moreover, a priority resolver is used to provide priority of application on the basis of two parameters, i.e., urgency and confidentiality. This priority resolver plays a very important role in the scheduling of jobs, as the information from sensor networks, i.e., the incoming data may have different priorities. As a matter of fact, only selected few users may have the right to initiate urgent requests, whereas others may just be allowed to propagate a routine request. The information tagged with these two parameters, viz., urgency and confidentiality, is handed over to the service handler, which checks for a requirement of use of interlinking service vertical. Otherwise, the three verticals work independent of each other using the resources made available to them. In a situation where a resource or a service is to be utilized from a vertical other than the one on which the application is run, the interservice communication module is affected.

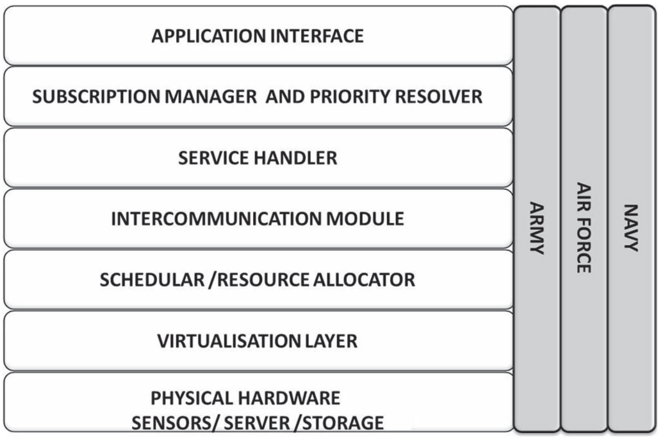

Fig. 4. Layered architecture of Mils-Cloud.

The intercommunication module acts as a gateway for an application to switch among the verticals for services and resources. In essence, the emphasis on the intercommunication module is the core for the implementation of sensor-cloud in an interservice cooperation for operations and decision making. The task is then scheduled for the service request on hardware on the basis of priority. Resources are allocated to the service request by the scheduler and the resource allocator. Let us take a scenario for the implementation of this infrastructure on a cloud. We propose that there are data centers divided for locations performing the role of the sensor network controller. Many users try to access the data generated by sensors. Hence, whoever requests for the sensor first are virtualized in that particular data center, and if the capacity is full for a data center, either the sensor gets virtualized on the next data center available or the user waits for some job that is getting executed to finish and then gets the VM. However, a noteworthy point is that both cases lead to delay either by waiting or getting on to another data center, thereby increasing network delays. In a typical military scenario, there typically exists a priority user who should be provided with this service without delays. The next task is to ensure that the priority user gets the service of a sensor without delay. This can be done by reserving some space in the data centers for priority users so that they get serviced promptly. However, the maximum amount of space to be reserved for priority users has to be worked out to some optimum level such that the normal users do not waste time due to idle data center resources waiting for priority users. The optimization problem can be formulated as follows:

$$\begin{aligned}&\text{Minimize } d\\&\quad\text{Such that}\\&R_i < \chi \quad \text{where} \quad i = 1, 2, 3 \ldots n\\&P_j \to 1 \quad \text{where} \quad j = 1, 2, 3 \ldots m.\end{aligned} \tag{10}$$

In (10), d is the delay in allocation of VM to a user. R_i is the percentage of resources reserved in the ith data center. χ is the percentage value of resources reserved. P_j is the probability that the jth user gets a VM in the required data center.

V. Challenges

The projected usage-related challenges of sensor-cloud in a military environment are as follows.

1) *Bandwidth*. It is a big challenge in providing bandwidth for fast data transfer in far forward areas in military operations. For migrating large objects, there is a substantial requirement of bandwidth. Some techniques for data fusion, data aggregation, and filtering unwanted data at the sensor network level may be used to overcome this problem by reducing the bandwidth requirement for transferring the sensor data, i.e., reducing the data flow from the sensor network to the cloud.
2) *Security*. Security is the primary concern for any military deployment. Data at one place are prone to physical attacks and cyber attacks. If someone gets access to data, the entire defense structure becomes transparent to him/her as there are very high chances that deployment and plans will be available on digital maps and documents on the sensor-cloud. Moreover, by keeping track of the information flows, areas of interest and activities can be monitored.
3) *Private cloud*. It may not provide all the advantages of CC in terms of cost effectiveness and may not be able to provide in true sense what is called infinite scalability.
4) *High fault tolerance*. There is little tolerance of a fault during any military operation. As such, a situation involving fault may collapse the entire command control structure. There is a need to have a high degree of reliability and redundancy, so that the command control structure failure does not come to a halt.
5) *Heterogeneity*. A sensor-cloud for military application should be capable enough to integrate different types of sensors in terms of complexity, handling power issues, storage, and easy usability. It should also be able to provide a common network interface to access storage and processing capabilities of cloud to retrieve sensed data from different sensors.
6) *Interference reduction*. WSNs mostly use wireless connectivity for data communication. The wireless links should be capable enough to handle interference and increase the collaboration of sensor nodes with other networked devices on the cloud. This is to ensure that the sensor nodes continue to function properly, and their efficiency of consistent data transmission is not compromised in the presence of other devices.
7) *Massive scale and real-time processing*. The integration of heterogeneous WSNs becomes even more challenging when there is a massive influx of sensed data that is required to be processed in real time.

VI. Simulation Analysis

The literature on performance parameters such as network latency, load sharing, cost, etc., that may be used for CC is available [19]–[21]. The scope of this work entails the development of sensor-cloud architecture for the integration of tri-services and the implementation of the cloud architecture on a CloudSIM simulator. Further, it is important to determine the efficiency of the architecture based on a set of performance parameters. CloudSIM [18] provides a platform for simulation of cloud-based infrastructure, which can be used for research activities. The simulation setup in CloudSIM consists in implementing the proposed hierarchical model of sensor-cloud. CloudSIM uses a BRITE file to model a network topology and various nodes and edges along with their parameters. We model three cloud brokers as users (army, navy, and air force), which are the starting nodes, and the data centers as the sensor network controllers, which are represented by leaf nodes, and the sensor cloud scheduler is modeled by the VM allocation policy class. Within the data centers, there are hosts that represent physical machines. There exists VMs that are virtual machines on this host. VMs are used to model sensors in the case of simulation. A user requests a service/application in the cloud. Then, a cloudlet is run on a virtual machine representing an application. In our setup, we use six cloudlets running on six VMs. Hence, when a user requests an application, it is received by the sensor-cloud scheduler, which is responsible for allocating the sensor network controller to the application, which gives access to the required sensors. The sensor network controllers 1, 2, 3, and 4 are controlling the sensor networks in locations A, B, C, and D, respectively. For simulation purposes, we scale down the capacity of a data center such that it can take a very limited number of VMs. The six sensors that need to be accessed by a user are located in the geographical location that is controlled by sensor network controller 1. However, in this case, sensors 1 and 2 are virtualized by sensor network controllers 1, 3, and 4; by sensor network controller 2; and so on. On running the simulation, we get the results summarized in Table I. In the results, VM ID $0, 1, \ldots, 5$ correspond to sensor $1, 2, \ldots, 6$. Data center ID 2, 3, 4 correspond to sensor network controllers 1–3.

Ideally, all of the six sensors should have been virtualized under sensor network controller 1 as per their geographical grouping. However, because of the limited capacity of sensor network controller 1, there were not enough resources available to virtualize the next four sensors. Therefore, they had to be virtualized on some other sensor network controller. Due to the unavailability of resources in sensor network controller 1, the sensor cloud scheduler has to fend for some other sensor

TABLE I
LATENCY DUE TO CONFIGURATION IN MILS-CLOUD

Cloudlet ID	Datacentre ID	VM ID	Start Time
0	2	0	49.3
1	2	1	49.3
2	3	2	52.3
3	3	3	52.3
4	4	4	53.3
5	4	5	53.3

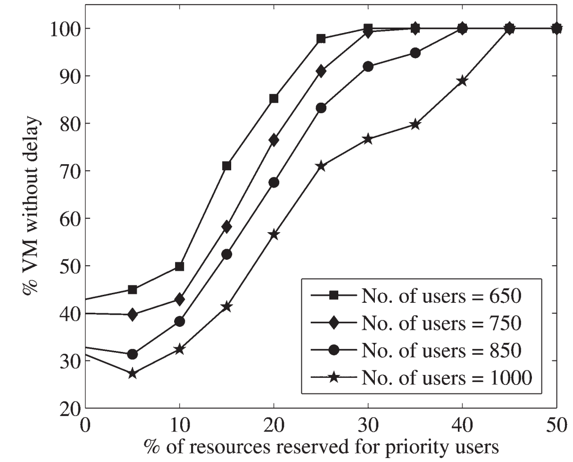

Fig. 5. Varying total number of users.

network controller to achieve the same. This causes latency in formation of a VM and, consequently, receipt of the sensed data because of processing and network delays. The usage of cloud resources is found using the cost of the usage model given in CloudSIM. In our simulation, the cost of usage for all the three data centers is the same, because we assume homogeneous sensor networks. However, if we deploy sensor networks that are heterogeneous in nature, the cost of usage will be different.

The next set of experiments includes simulation of delay guarantee to the priority user and results to indicate the percentage satisfaction of priority request being serviced without delay. In this set of experiments, we try to observe the results of reserving some resources in a data center, so as to facilitate the access of priority users without delay. The scenario here is that there are a certain number of priority users randomly generated and how efficiently in a data center their requests can be accommodated. In the simulation, we generate requests for access to sensor data by both normal and priority users. The occurrence of a priority user is given as a probability from the total number of users and generated randomly. Under a normal circumstance, all the requests are handled on a first-come–first-serve basis and in a critical condition when the sensor network controller is out of resources; in such a case, the priority user will have to be in a situation where they get delayed information. However, if we modify this approach by reserving some resources for priority users, we may avoid such a situation. Timely information is of utmost importance to the priority users who are commanders at different levels so as to enable them to exercise their command and control in an effective manner. Fig. 5 shows the simulation results of variation in the number of users after reserving some percentage of space in sensor network controllers while keeping the number of hosts per data center and the number of cores per host constant. As we can see, there are limited resources with the sensor network controller, and advantage of reserving is achieved up to a level of 25%–30% of resources for 750 users. Thereafter, access to VMs is 100%, and reserving beyond that leads to wastage of resources. Moreover, the graph shows a downward trend in percentage satisfaction of priority users as we increase the number of users.

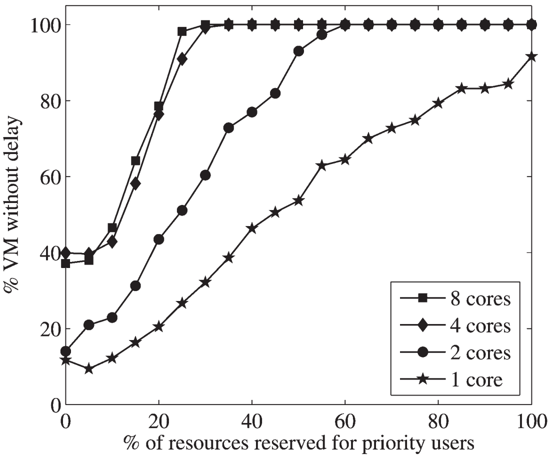

Fig. 6. Varying the capacity of data center.

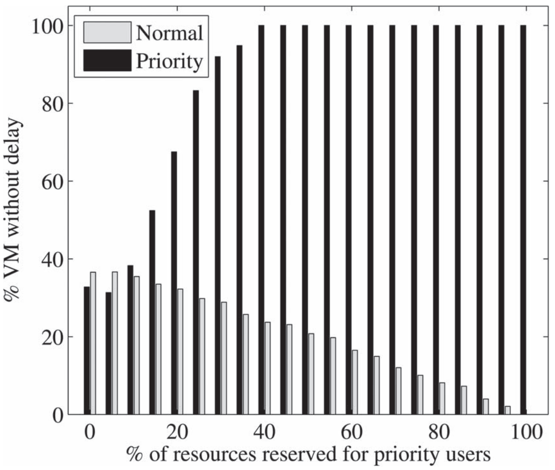

Fig. 7. Comparison priority versus normal users.

In Fig. 6, the plot shows delay performance with variation in capacity of data center, i.e., varying the number of cores in a host and keeping the rest of the parameters constant. In a resource-constraint data center, even after reserving 100%, we may not achieve 100% satisfaction for priority users due to shortage of capacity of data center. In Fig. 7, we show a comparison of normal and priority users with increasing reservation of resources in two different scenarios. From the simulations carried out, it is evident that an optimum value of resources reserved leads to a maximum satisfaction of priority users. Beyond a certain limit of reservation in each scenario, there is waste of resources and increase in the delay of normal users without further benefiting the priority users. In Fig. 8, if we increase the probability of requests of priority users, the graph shifts right with increasing probability. This behavior is exhibited due to the increase in the number of priority users, as the probability of their occurrence increases.

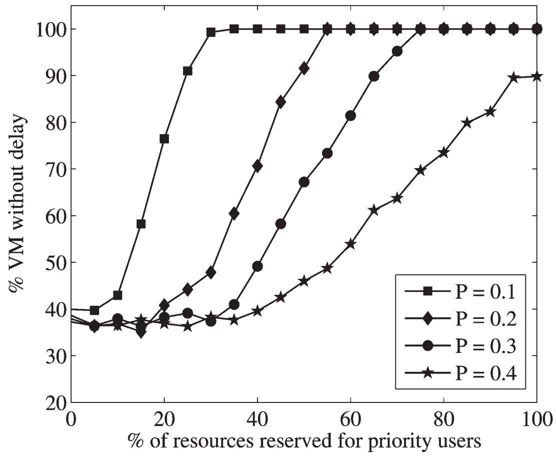

Fig. 8. Varying probability (P) of priority users.

VII. Conclusion

The recent research on sensor-cloud technologies focus on formulation of policies, system, and new methods for efficient usage of sensor-cloud infrastructure. The system described in this paper attempts to provide a platform to configure and implement defense applications based on WSNs on the cloud. The system provides scalable and flexible access to resources, overcomes heterogeneity problems, and provides services to different users. This architecture aims at providing a platform for military tri-services cooperation in decision making and operations. The employment of sensor-cloud for military applications has tremendous scope of growth. This is an emerging field of research, and many interesting applications can be derived for enhancing the effectiveness of defense forces. After the implementation of the sensor-cloud infrastructure on the CloudSIM simulator, future works in this direction include the following: 1) Formulating an optimization strategy for virtualization of sensors with respect to their availability and data processing at sensors or cloud infrastructure, keeping in mind the availability of bandwidth. This is because, in case of a limited-bandwidth environment, transmitting the entire sensor data to the sensor network controller would be a time-consuming process with losses. However, we save on the processing power at the sensor nodes, thereby increasing the battery life of a sensor. Therefore, a need arises for an optimal strategy for the same. 2) A strategy for dynamically allocating the virtual and physical sensors, processing, and storage resources in case of an overload, or in an event of a failure, keeping in view the location-based grouping of sensor resources. 3) Policy for minimizing access time of data by the three verticals from cloud infrastructure. 4) A cloud-based recommender system [22] based on tri-services sensor data may be developed. 5) Finally, considering the dynamic nature of military operations and the associated decision making, adaptive learning mechanisms (such as those based on Learning Automata [23] or Markov decision processes [24]) may be incorporated into the proposed system. The aforementioned issues need to be explored for firming up the proposed architecture, the associated infrastructure, and its performance evaluation. Moreover, there is a requirement to tune bottlenecks, if there is any found during the implementation.

References

[1] A. Alamri, W. S. Ansari, M. M. Hassan, M. S. Hossain, A. Alelaiwi, and M. A. Hossain, “A survey on sensor-cloud: Architecture, applications, and approaches,” *Int. J. Distrib. Sensor Netw.*, vol. 2013, pp. 917923-1–917923-18, 2013.

[2] R. Buyya, C. S. Yeoa, S. Venugopala, J. Broberga, and I. Brandic, “Cloud computing and emerging it platforms: Vision, hype, and reality for delivering computing as the 5th utility,” *Future Gener. Comput. Syst.*, vol. 25, no. 6, pp. 599–616, Jun. 2009.

[3] [Online]. Available: www.militaryaerospace.com/articles/2012/08/tactical-cloud-computing.htm

[4] [Online]. Available: http://www.disa.mil/Services/Enterprise-Services/Infrastructure/RACE

[5] M. Yuriyama and T. Kushida, “Sensor-cloud infrastructure—Physical sensor management with virtualized sensors on cloud computing,” in *Proc. 13th IEEE Int. Conf. Netw.-Based Inf. Syst.*, Sep. 14–16, 2010, pp. 1–8.

[6] P. Wittek and X. Rubio-Campillo, “Military reconstructive simulation in the cloud to aid battlefield excavations,” in *Proc. 4th IEEE Int. Conf. CloudCom*, Dec. 3–6, 2012, pp. 869–874.

[7] V. Rajesh, O. Pandithurai, and S. Mageshkumar, “Wireless sensor node data on cloud,” in *Proc. IEEE ICCCCT*, Oct. 7–9, 2010, pp. 476–481.

[8] X. Cheng and X. Liao, “The application of cloud computing in military intelligence fusion,” in *Proc. Int. Conf. Inf. Technol., Comput. Eng. Manag. Sci.*, Sep. 24–25, 2011, pp. 241–244.

[9] W. Q. Wang, X. Zhang, J. Zhang, and H. B. Lim, “Smart traffic cloud: An infrastructure for traffic applications,” in *Proc. 18th IEEE Int. Conf. Parall. Distrib. Syst.*, Dec. 17–19, 2012, pp. 822–827.

[10] G. Fortino, M. Pathan, and G. D. Fatta, “BodyCloud: Integration of cloud computing and body sensor networks,” in *Proc. 4th IEEE Int. Conf. CloudCom*, Dec. 3–6, 2012, pp. 851–856.

[11] C.-F. Lai, H. Wang, H.-C. Chao, and G. Nan, “A network and device aware QoS approach for cloud-based mobile streaming,” *IEEE Trans. Multimedia*, vol. 15, no. 4, pp. 747–757, Jun. 2013.

[12] C.-F. Lai, Y.-X. Lai, H.-C. Chao, and J. Wan, “Cloud-assisted real-time transrating for http live streaming,” *IEEE Wireless Commun. Mag.*, vol. 20, no. 3, pp. 62–70, Jun. 2013.

[13] S.-Y. Chen and Y.-M. Huang, “Establishment and application for a mobile learning communities system over cloud network: A case study of digital archives resource into outdoor environmental education,” *J. Internet Technol.*, vol. 14, no. 6, pp. 985–996, Nov. 2013.

[14] A. L. Zhou and H. Wang, “Toward blind scheduling in mobile media cloud: Fairness, simplicity, and asymptotic optimality,” *IEEE Trans. Multimedia*, vol. 15, no. 4, pp. 735–746, Jun. 2013.

[15] B. L. Zhou, X. Wang, W. Tu, G. Mutean, and B. Geller, “Distributed scheduling scheme for video streaming over multi-channel multi-radio multi-hop wireless networks,” *IEEE J. Sel. Areas Commun.*, vol. 28, no. 3, pp. 409–419, Apr. 2010.

[16] T. Kobialka, R. Buyya, C. Leckie, and R. Kotagiri, “A sensor web middleware with stateful services for heterogeneous sensor networks,” in *Proc. 3rd Int. Conf. Intell. Sens., Sens. Netw. Inf.*, Dec. 3–6, 2007, pp. 491–496.

[17] A. di Costanzo, M. D. de Assuncao, and R. Buyya, “Harnessing cloud technologies for a virtualized distributed computing infrastructure,” *IEEE Internet Comput.*, vol. 13, no. 5, pp. 24–33, Sep./Oct. 2009.

[18] R. N. Calheiros, R. Ranjan, A. Beloglazov, C. A. F. D. Rose, and R. Buyya, “CloudSim: A toolkit for modeling and simulation of cloud computing environments and evaluation of resource provisioning algorithms,” *Softw., Pract. Experience*, vol. 41, no. 1, pp. 23–50, Jan. 2011.

[19] A. Iosup, S. Ostermann, N. Yigitbasi, R. Prodan, T. Fahringer, and D. Epema, “Performance analysis of cloud computing services for many-tasks scientific computing,” *IEEE Trans. Parall. Distrib. Syst.*, vol. 22, no. 6, pp. 931–945, Jun. 2011.

[20] S. Misra, P. V. Krishna, K. Kalaiselvan, V. Saritha, and M. S. Obaidat, “Learning automata-based QoS framework for cloud IaaS,” *IEEE Trans. Netw. Serv. Manag.*, Feb. 2014, doi: 10.1109/TNSM.2014.011614.130429.

[21] L. Babu and P. V. Krishna, “Honey bee behavior inspired load balancing of tasks in cloud computing environments,” *Appl. Soft Comput.*, vol. 13, no. 5, pp. 2292–2303, May 2013.

[22] P. V. Krishna, S. Misra, D. Joshi, and M. S. Obaidat, “Learning automata based sentiment analysis for recommender system on cloud,” in *Proc. IEEE Int. Conf. CITS*, May 7/8, 2013, pp. 1–5.

[23] S. Misra, V. Tiwari, and M. S. Obaidat, “LACAS: Learning automata-based congestion avoidance scheme for healthcare wireless sensor networks,” *IEEE J. Sel. Areas Commun.*, vol. 27, no. 4, pp. 466–479, May 2009.

[24] S. Misra, S. V. R. Mohan, and R. Choudhuri, “A probabilistic approach to minimize the conjunctive costs of node replacement and performance loss in the management of wireless sensor networks,” *IEEE Trans. Netw. Serv. Manag.*, vol. 7, no. 2, pp. 107–117, Jun. 2010.

Sudip Misra is an Associate Professor in the School of Information Technology at the Indian Institute of Technology Kharagpur, Kharagpur, India. Prior to this he was associated with Cornell University, Ithaca, NY, USA, Yale University, New Haven, CT, USA, Nortel Networks, Mississauga, ON, Canada and the Government of Ontario (Canada). He received the Ph.D. degree in Computer Science from Carleton University, Ottawa, ON, and the Masters and Bachelors degrees respectively from the University of New Brunswick, Fredericton, NB, Canada, and the Indian Institute of Technology, Kharagpur, India. He has several years of experience working in the academia, government, and the private sectors in research, teaching, consulting, project management, architecture, software design and product engineering roles.

His current research interests include algorithm design for emerging communication networks. He is the author of over 180 scholarly research papers (including 90 journal papers). He has won eight research paper awards in different conferences. He was awarded the IEEE ComSoc Asia Pacific Outstanding Young Researcher Award at IEEE GLOBECOM 2012, Anaheim, California, USA. He was also the recipient of several academic awards and fellowships such as the Young Scientist Award (National Academy of Sciences, India), Young Systems Scientist Award (Systems Society of India), Young Engineers Award (Institution of Engineers, India), (Canadian) Governor Generals Academic Gold Medal at Carleton University, the University Outstanding Graduate Student Award in the Doctoral level at Carleton University and the National Academy of Sciences, India Swarna Jayanti Puraskar (Golden Jubilee Award). He was also awarded the Canadian Governments prestigious NSERC Post Doctoral Fellowship and the Humboldt Research Fellowship in Germany. He is the Editor-in-Chief of the International Journal of Communication Networks and Distributed Systems (IJCNDS), Inderscience, U.K. He has also been serving as the Associate Editor of the Telecommunication Systems Journal (Springer), Security and Communication Networks Journal (Wiley), International Journal of Communication Systems (Wiley), and the EURASIP Journal of Wireless Communications and Networking. He is also an Editor/Editorial Board Member/Editorial Review Board Member of the IET Communications Journal, IET Wireless Sensor Systems, and Computers and Electrical Engineering Journal (Elsevier). He has edited 6 books in the areas of wireless ad hoc networks, wireless sensor networks, wireless mesh networks, communication networks and distributed systems, network reliability and fault tolerance, and information and coding theory, published by reputed publishers such as Springer, Wiley, and World Scientific. He was invited to chair several international conference/workshop programs and sessions. He served in the program committees of several international conferences.

Dr. Misra was also invited to deliver keynote/invited lectures in over 20 international conferences in USA, Canada, Europe, Asia and Africa.

Anuj Singh is presently working toward Master of Technology in information technology from the School of Information Technology, Indian Institute of Technology, Kharagpur, India. He completed the B.Tech. degree in electronics engineering from Jawaharlal Nehru University, New Delhi, India, in 2009.

His current research interests are Wireless Sensor Networks, Cloud Computing and Sensor-Cloud.

Subarna Chatterjee is presently working as a Junior Research Fellow and working toward the Ph.D. degree from the School of Information Technology, Indian Institute of Technology, Kharagpur, India. She received the B.Tech. degree in computer science and technology from West Bengal University of Technology, Kolkata, India, in 2012. Her current research interests include networking and communication aspects of Cloud Computing in Wireless Sensor Networks.

Mohammad S. Obaidat (S'85–M'86–SM'91–F'05) received the Ph.D. and M. S. degrees in computer engineering with a minor in computer science from The Ohio State University, Columbus, Ohio, USA.

He is currently a Full Professor in computer science and software engineering with Monmouth University, NJ, USA, where he previously served as the Chair of the Department of Computer Science and the Director of the Graduate Program. He was a Faculty Member with the City University of New York, New York, NY, USA. During 2004–2005, he was on sabbatical leave as a Fulbright Distinguished Professor and Advisor to the President of Philadelphia University Jordan, Amman, Jordan, i.e., Dr. Adnan Badran, who was the Prime Minister of Jordan in April 2005 and served earlier as the Deputy Director General of the United Nations Educational, Scientific and Cultural Organization. He has received extensive research funding and has published about 30 books and over 600 refereed technical articles in scholarly international journals and proceedings of international conferences. He served as a consultant for several corporations and organizations worldwide. His research interests include wireless communications and networks, telecommunications and networking systems, security of network, information and computer systems, security of e-based systems, performance evaluation of computer systems, algorithms and networks, green information and communications technology, smart homes and cities, high-performance and parallel computing/computers, applied neural networks and pattern recognition, and adaptive learning and speech processing.

Prof. Obaidat is a Fellow of the Society for Modeling and Simulation International (SCS). He was a recipient of the Nokia Research Fellowship; the Distinguished Fulbright Scholar Award; the SCS Outstanding Service Award for his excellent leadership, services, and technical contributions; the McLeod Founder's Award in recognition of his outstanding technical and professional contributions to modeling and simulation; the IEEE Global Communications Conference (GLOBECOM) 2010 Outstanding Leadership Award from the IEEE Communications Society for his outstanding leadership in the Communication Software Services and Multimedia Applications Symposium (CSSMA 2010); the SCS Presidential Service Award for his outstanding, unique, and long-term technical contributions and services to the profession and society. He was also a recipient of several awards for his papers in international conferences, such as IEEE GLOBECOM; IEEE Arab Computing Society International Conference on Computer Systems and Applications (AICCSA); IEEE International Conference on Data Communication Networking; IEEE International Conference on Computer, Information, and Telecommunication Systems (CITS); etc. Between 1994 and 1997, he has served as a Distinguished Speaker/Visitor of IEEE Computer Society. Since 1995, he has been serving as an ACM Distinguished Lecturer. He is also an SCS Distinguished Lecturer. Between 1996 and 1999, he served as an IEEE/ACM Program Evaluator of the Computing Sciences Accreditation Board/Commission (CSAB/CSAC). Between 2009 and 2011, he served as the President of the SCS. He also has served as SCS Senior Vice President (VP), VP Conferences, and VP Membership. He is the Editor-in-Chief of three scholarly international journals. He is also an editor and advisory editor of numerous journals and transactions. He has guest edited numerous special issues of scholarly journals, such as IEEE TRANSACTIONS ON SYSTEMS, MAN AND CYBERNETICS (SMC), IEEE WIRELESS COMMUNICATIONS, IEEE SYSTEMS JOURNAL, *SIMULATION: Transactions of SCS, Elsevier Computer Communications Journal, Journal of Computers and Electrical Engineering, Wiley Security and Communication Networks, Journal of Networks*, and *International Journal of Communication Systems*, among others. He served as the Steering Committee Chair, Advisory Committee Chair, and Program Chair of numerous international conferences. He is the founder of two well-known international conferences: International Symposium on Performance Evaluation of Computer and Telecommunication Systems (SPECTS) and CITS. He has chaired numerous international conferences and has given numerous keynote speeches worldwide.