# Relevance of Cloud Computing for Defence

***Ajey Lele* and Munish Sharma*****

*Technology has always played the key role in defining the outcome of war. A modern-day military is investing in cutting-edge technologies to leverage their benefits in the evolving nature of warfare, which encompasses every aspect of science. In the case of information and communication technology (ICT), the research and development has unleashed vast potential for civilian and military applications, which vary from simple logic execution to high-end supercomputing. As cloud computing has made inroads in the operations of private sector, it is slated to perform a central role in the functioning of governments and defence and security agencies. Under the aegis of ICT, the emerging cloud computing can find applications in defence sector as it offers numerous advantages over traditional information technology (IT) systems such as scalability, agility and interoperability. The article is an attempt to identify the key defence operations where cloud computing could help in addressing the IT needs while keeping the acquisition and maintenance costs at minimal. It brings in the concerns and challenges lying ahead in the way of adopting cloud computing while taking stock of initiatives taken by the governments of leading militaries of the world.*

> I don't need a hard disk in my computer if I can get to the server faster…carrying around these non-connected computers is byzantine by comparison.
>
> Steve Jobs (1997)

* Ajey Lele is a Research Fellow at Institute for Defence Studies and Analyses, New Delhi.
** Munish Sharma is a Research Assistant at Department of Geopolitics and International Relations, Manipal University.

*ISSN 0976-1004 print*

*Journal of Defence Studies, Vol. 8, No. 2, April–June 2014, pp. 63–84*

Technology has always been an important part of any war. The war fighting capabilities of nation-states are dictated by the nature of technologies available in those periods. In the twenty-first century, the emergence of hybrid and irregular warfare over and above the conventional threat demands upgrading and addition of newer military technologies. For any nation-state, it is important to provide their armed forces and national security agencies with the best capabilities to enable them to protect the state's long-term and short-term interests.

With the advent of Revolution in Military Affairs (RMA), new operational concepts and doctrines are evolving. Various modern technologies like nanotechnology, robotics, life sciences and bio-technology are impacting the RMA. In particular, technologies related to the cyber and space are making a significant impact and states are preparing themselves to fight in a digitized battlefield environment. Various developments in the field of information and communication technologies (ICT) are quickly realizing a place into the state's security architecture. Overall, cyberspace is a complex, rapidly changing yet real-time and increasingly interconnected technological domain. Progressions in ICT are also directly or indirectly impacting various security architectures. Security agencies are embracing several new technological additions (both hardware and software). This article discusses one such addition to the field of computing—cloud computing—and its impact on the security architecture.

## What is Cloud Computing?

Cloud computing is akin to the electricity industry where every consumer is not the custodian of any major power grid network but draws electricity as per requirement from a wider electricity apparatus. Essentially, it is about the sharing of resources. For running any application on a computer, help is sought from the network of computers that make up the cloud. Hence, the hardware and software needs of the user reduce drastically. What the user requires is a reasonably 'modern' computer capable of doing standard operations and able to interact with the remote cloud organization. In broad terms, any user using e-mail servers like Yahoo or Google mail is provided interconnectivity by operating computational services from the 'cloud'.

The concept of cloud computing is not new; it has its roots in the mainframe, client-server and Internet era, which gave consumers the freedom of access from any location with an Internet connection. The

applications, servers and data centres are maintained by the service provider and the consumer pays for the services availed. Major corporations, including Amazon, Google, IBM, Sun, Cisco, Dell, HP, Intel, Novell and Oracle, have invested in cloud computing and offer individuals and businesses a range of cloud-based solutions. The users can access their applications and data from any location at any time with minimal hardware requirements to execute the middleware. The processing and data storage takes place at the provider's end. For individual applications, e-mail, YouTube, Flickr, Panoramio, Google Docs, slideshare and Dropbox are examples of cloud computing for image, video and document storage and processing.

As per the definition of the United States' National Institute of Standards and Technology, 'Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.'[1] The cloud user—be it an individual or an organization—is able to scale up or down usage and resources in the real time for any variations in the demand. The user does not need to forecast the usage or allocate resources in advance. The very concept of shared pool of resources gives the user the advantage of provisioning computing resources whenever there is surge in demand, enabling the continuation of services without the need to procure hardware or software and without the concerns of resources lying idle for a long duration. Furthermore, cloud computing enables the consumer to scale up or expand their IT infrastructure without any investment in hardware, software licensing and human resources. Unlike traditional systems, the user of cloud computing need not be in the same location as the data storage.

Cloud computing services are delivered through a network, usually the Internet. The cloud architecture is composed of five essential characteristics—on-demand self-service, broad network access, resource pooling, rapid elasticity and measured service; four deployment models—private, community, public and hybrid—and three service models. The service models of cloud providers differ in the amount of control the users have over information and could be described as:[2] Infrastructure-as-a-Service (IaaS); Platform-as-a-Service (PaaS); and Software-as-a-Service (SaaS). The three service models or layers are completed by an end user

layer that encapsulates the end user perspective on cloud services. The model is shown in Figure 1.

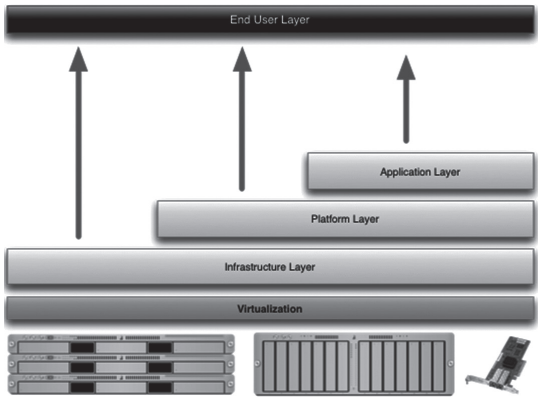


**Figure 1** Service Models and End User Layer

*Source:* http://www.cloud-competence-center.com/understanding/cloud-computing-service-models/, accessed on 21 March 2014.

## SaaS

Software-as-a-Service provides complete applications to a cloud's end user. It is mainly accessed through a web portal and service-oriented architectures based on web service technologies (see Figure 2). The cloud

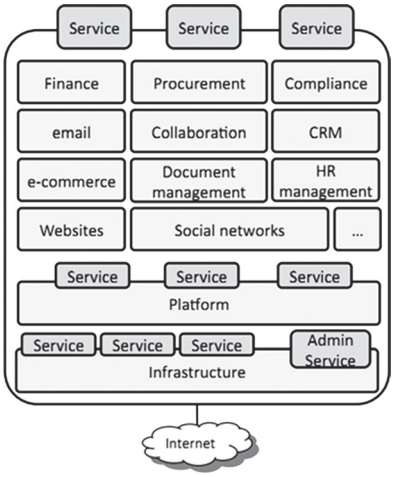


**Figure 2** Software-as-a-Service (SaaS) Stack

*Source:* http://www.cloud-competence-center.com/understanding/cloud-computing-service-models/, accessed on 21 March 2014.

infrastructure, such as network, servers, storage devices, applications and operating systems, is not managed by the consumer. Examples of SaaS vendor services include Salesforce.com Customer Relationship Management (CRM), Google Docs, Gmail and Microsoft Office 365.

**PaaS**

PaaS comprises the environment for developing and provisioning cloud applications. The principal users of this layer are developers seeking to develop and run a cloud application for a particular platform. They are supported by the platform operators with an open or proprietary language; a set of essential basic services to facilitate communication, monitoring or service billing; and various other components, for instance, to facilitate start-up or ensure an application's scalability and/or elasticity (see Figure 3).

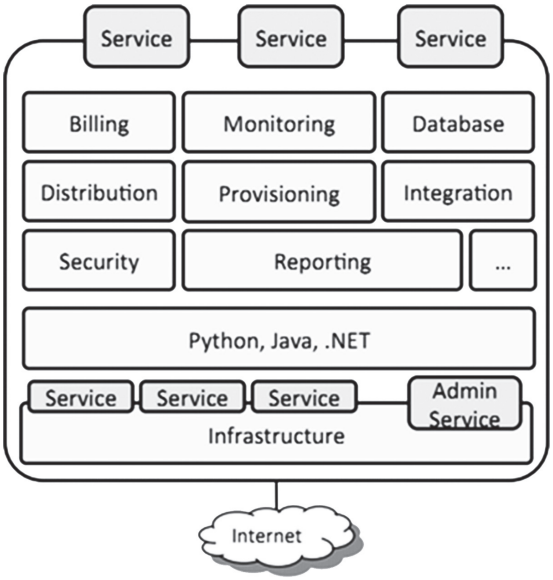


**Figure 3** Platform-as-a-Service (PaaS) Stack

*Source:* http://www.cloud-competence-center.com/understanding/cloud-computing-service-models/, accessed on 21 March 2014.

Basically, in this case, cloud infrastructure is managed by the provider, while the consumer has control over the configuration settings and application life cycle. Examples of PaaS vendor services include Google App Engine, Force.com, Amazon Web Services Elastic Beanstalk and the Microsoft Windows Azure platform.

**IaaS**

The services on the infrastructure layer are used to access essential IT resources that are combined under the heading IaaS. These essential IT resources include services linked to computing resources, data storage resources and the communications channel. Physical resources are abstracted by virtualization, which means they can then be shared by several operating systems and end user environments on the virtual resources—ideally, without any mutual interference. These virtualized resources usually comprise central processing unit (CPU) and random access memory (RAM), data storage resources (elastic block store and databases) and network resources as displayed in Figure 4.

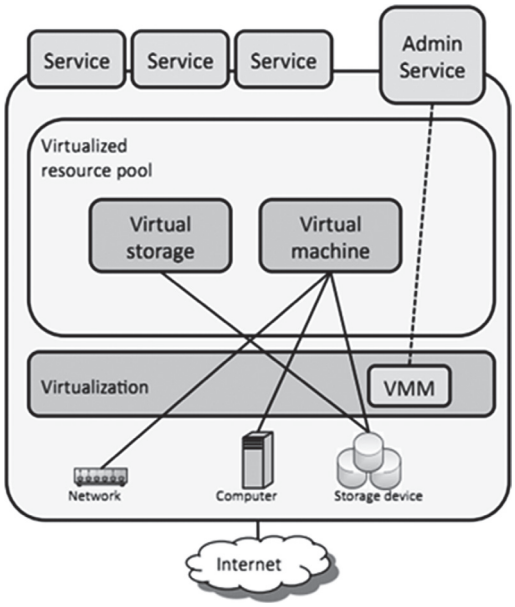


**Figure 4** Infrastructure-as-a-Service (IaaS) Stack

Source: http://www.cloud-competence-center.com/understanding/cloud-computing-service-models/, accessed on 21 March 2014.

The consumer of IaaS has control over operating systems, storage and applications, and limited control of select networking components, such as firewalls. The consumer has no role in the management or control of cloud infrastructure. Examples of IaaS vendor services include Amazon Elastic Compute Cloud (EC2), GoGrid and Rackspace Cloud.

Overall, cloud computing is a result of the convergence of grid

computing, utility computing and SaaS. It essentially represents the increasing trend towards the external deployment of IT resources, such as computational power, storage or business applications, and obtaining them as services.[3] The demand and business for cloud computing is primarily propelled by the economies of scale made available due to large-scale computational infrastructure; the ability to manage surge or decline in demand; and the meta-data availability for analytics. Once cloud is adopted, the organization does not need to manage software installations and upgrades, or maintain IT support functions, testing and deployment cycles or in-house set of developers. New projects require upfront hardware investment and if usage increases new hardware must be added. In the case of cloud, the organization does not need to plan for additional hardware requirements.

The three cloud deployment models have different security requirements due to varying environment. For instance, IaaS is the foundation of all cloud services, with PaaS built upon it and SaaS, in turn, built upon the other two. Just as capabilities are inherited, so are the information security issues and risks. If the cloud service provider takes care of only the security at the lower part of the security architecture, the consumers become more responsible for implementing and managing the security capabilities.[4]

## Future Trajectory and Applications of Cloud Computing

Cloud computing has already made inroads into various business arenas and is expected to play an increasingly important role in the business and governmental sectors in the near future. Various surveys conducted in this context depict a great potential for development of this technology. The use of cloud computing is growing at a compound annual growth rate of 26 per cent globally and is expected to account for 20 per cent of global IT market, excluding IT services and client devices, by 2015.[5] It has been estimated that worldwide cloud computing will reach a market size of approximately US$ 20 billion by 2016.[6] A World Economic Forum report indicates that cloud computing is going to help enterprises of all sizes and government institutions in both emerging and established economies to increase productivity and address major health care, education and societal issues.[7] Cloud technology already has numerous applications for individuals, business ventures and governmental organizations, and with the further developments in technology, more applications are expected to materialize.

The dynamic nature of business processes raises the need for agility in operations and ease of scalability as the demand surges. Cloud computing can help address these issues as well as increase productivity and ensure business continuity at a greatly optimized cost. In the case of enterprises, functions such as virtual office, payroll, CRM, human resources management (HRM), enterprise resource planning (ERP), supply chain management (SCM), analytics and project management are executed over cloud.

Traditional IT systems are capital intensive, which remains a challenge for governments in developing economies. The solution lies in cloud computing as it leverages common infrastructure of government agencies for resource sharing and cost optimization.

Cloud computing could lead to faster and more efficient implementation of upgrades and other technological advances. It offers a possibility to provide innovators with a broader range of scalable tools for research, development and testing than they would be able to acquire cost effectively for a local computing environment.[8] Furthermore, the technology is viewed as more reliable due to distributed architecture and redundancy built between the computing resources.

## Cloud Computing for Defence Applications

Hitherto, it was observed that new technologies first make inroads into the defence arena and subsequently find their way into the civilian domain. The origins of IT, and particularly that of the Internet, can be found in defence domains. However, future developments in these technologies, particularly that of application-oriented techniques, have mostly occurred in the civilian domain; it is the same case with cloud computing.

Over the years, the armed forces' dependence on ICT has increased significantly. Availability of data in real time (network-centric battlefield) is the main requirement for modern militaries. At the same time, ever-increasing financial constraints are leading defence agencies towards cost saving in general. 'Cloud' offers best option for the requirements of modern militaries. Some militaries have started incorporating cloud computing in their systems, while others are still in the process of identifying the possible options.

Generally, it has been observed that the defence systems are built based on the need of the mission, thus the IT architecture has limited interoperability. Moreover, in case of large defence organizations, there are many mission-oriented systems which have never been tried or tested

to work in cohesion with each other.[9] The IT resources thus developed do not run at optimum levels or stay idle during peacetime, which is the primary reason of inefficiency. The deployment of defence forces needs agility in the operations. Along with forces, computing resources are also deployed, which need to be agile as well. All this indicates that there is a scope and need for making good use of existing resources with some modifications and cloud computing offers an option in this regard.

Network centricity is emerging as a key element of defence transformation. The concept encapsulates the use of computers, high-speed data links and networks for exchange of data, software to link personnel on the ground, different platforms, and so on, into integrated local and wide area networks. The evolving nature of warfare, thus known as network-centric warfare (NCW), is the doctrine where forces utilize these networks, enabling the personnel to share large amounts of critical information in real time, thereby improving the combat capability and efficiency. The quantum of data being generated by the end users and input systems, such as intelligence, surveillance and reconnaissance (ISR), needs to be analysed using data fusion techniques and disseminated for decision making. This integration of platforms, spread across land, sea, air and cyberspace, paves the way for an operating model for large, geographically spread organizations to have enhanced situational awareness and a united, coordinated and synchronized decision-making process, which is critical in modern-day warfare. The future operating environment of NCW could be cloud computing.[10]

The defence operations that are likely to benefit from cloud computing are primarily those involving varying or unpredictable computing requirements, or the integration of many, high-capacity data feeds from sensor networks and other sources.[11] The applications requiring agility, scale out and the ability to integrate or analyse massive data are best fit to be considered for cloud-based computing solutions. Such applications include: big data analysis; intelligence integration; processing and dissemination of data gathered through ISR; large-scale modelling and simulation; and advanced decision support systems. As the defence missions integrate feeds from various sensors of ISR capability, missions may include the analysis of very large datasets. The high-resolution imagery generated by on-board sensors[12] flows round the clock; thus, it requires data centres for storage and high-speed computers for analysis and should be made available to different stakeholders at any given point of time. An additional benefit is the productivity gained from

a ubiquitous connection to common cloud-based services, such as e-mail, unclassified training or document preparation.

For defence forces, the basic fear for opting for cloud computing relates to the security of the system. This is because the cloud depends on multiple databases which could originate from different servers; moreover, there is always a threat of cyber attacks. Data security is therefore the major concern and organizations refrain from moving classified and mission-critical data to cloud due to the lack of trust in the security of the provider's environment. However, this does not mean that there are no remedies for this, at the same time, the chances of 'successful attack' would always exist. It would mostly depend on the priority of the military leadership about which 'arena' they would like to opt for induction of cloud.

Training is one such arena where the military leadership could find the maximum utility of the cloud. Defence organizations run massive knowledge management programmes in the form of education and training for the personnel at every stage of their careers, varying from induction to advanced specialized courses. With the advent of IT in classrooms, cloud can transform the way these courses are delivered to the soldiers spread across a wide geography. There are various ideas developed for civilian training domains (knowledge management). Organizations like Coursera, Accenture, TCS and Infosys have developed repository of technical and professional trainings available over the Intranet or Internet. Specific defence training modules could be developed on similar lines.

Accenture has worked on the operational methods and state in a report,[13]

> Cloud Computing could change the operational methods of defence agencies. Cloud Computing would enable strong security and resistance to cyber-attacks due to inherent consistency in implementation of standards. The applications for defence agencies were developed in silos with specific mission requirements, which open up the ground for vulnerabilities and a huge electronic surface to defend. The access and identity management systems are based on advanced biometric and geo-location authentication, as well as risk-based, adaptive authorization.

The report brings out the application of exploratory security analytics[14] to curb intrusion attempts. It is important to appreciate that military data gets generated in volumes from a vast array of sources, including satellites, air and ground reconnaissance and geopolitical and military intelligence

networks/agencies. This generated data needs to be stored, processed, shared and made available to the strategic planners and personnel on the ground for decision making.

In general, once the applications are integrated with cloud computing logic, the networks can attain increased flexibility, cost effectiveness, efficiency and accessibility. The networks and applications need to be resilient and secure with low restoration time due to their strategic significance.

For defence requirements, collaboration tools, e-mail, administrative applications, conferencing software, mission applications and specific applications used for programme or project management could be viewed as key areas, where there is a need to opt for a cloud. However, there appears to be some ambiguity in minds of military leadership to welcome cloud wholeheartedly. As per market research conducted by Lockheed Martin, 'the decision makers in IT are reluctant to move mission-critical data management, procurement, human resource management and financial management systems to cloud pertaining to security concerns.'[15]

Appreciating the importance of cloud computing for defence forces but, at the same time, factoring the discomfort of military establishments to opt for a fully cloud-driven digital battlefield management system, it is important to identify how best the cloud be intertwined in various military applications. Table 1 suggests a possible matrix in this regard.

## Cloud Computing in Defence: Global Canvas

Defence establishments from few developed states have already started making investments into the cloud systems. This section offers a brief overview about them.

### Cloud Computing in the United States (US) Department of Defense (DoD)

The IT dependence of the DoD is well known. Most of the US defence infrastructure is totally IT dependent, and even for an individual soldier on the battlefield, his decision-making capabilities are dependent on various real-time inputs received by him/her electronically. The development, operation and management of resources required for the management of the huge IT set-up is costly and also prone to interference (virus attacks, for example). Also, constant upgrades are required to manage and maintain the IT infrastructure.

The process of IT modernization remains dynamic. Presently, the

**Table 1** Defence Cloud with IaaS and PaaS Implementation Stack

<table>
<tr><td colspan="5">IaaS Implementation</td><td>PaaS Implementation</td></tr>
<tr><td rowspan="3">Equipment grid at land/sea/ air/space</td><td rowspan="3">1. Assessment, collation, planning, decision making at the command centre.<br>2. Dissemination to fixed/ deployable/ mobile units</td><td>Digital signal processing.<br>Image processing.<br>Geospatial and battlefield data integration.</td><td>Voice/video communication.<br>Geospatial data.<br>Messaging service.</td><td rowspan="2">Positioning and navigation.<br>Telemetry and control systems.<br>Electronic warfare.</td><td rowspan="4">Learning and Training.<br>Simulation/War-gaming.<br>Project Management.<br>Procurement/Inventory Management.<br>Supply Chain Management.<br>Human Resource Management.<br>Design/Development/ Visualization.<br>Email Services.</td></tr>
<tr><td>Intelligence data processing</td><td>Intelligence data sharing</td></tr>
<tr><td colspan="2">Battlespace awareness</td><td>Engagement</td></tr>
<tr><td>ISR</td><td>Command and control</td><td colspan="3">Battlespace management</td></tr>
<tr><td colspan="5">Network-centric Warfare</td><td>Other Defence Operations</td></tr>
<tr><td colspan="6">Implementation Layer</td></tr>
<tr><td colspan="3">Development tools and run time environment (Ada/Java/Assembly/C/C++/.NET)</td><td>Database</td><td>Middleware</td><td>Embedded Systems</td></tr>
<tr><td colspan="6">Platform Layer</td></tr>
<tr><td colspan="6">Memory CPU Storage Network Communication</td></tr>
<tr><td colspan="6">Infrastructure Layer</td></tr>
</table>

US DoD is addressing existing issues: suboptimal data centres leading to unnecessary costs; limited interoperability, reducing information sharing and mission collaboration; and the long time taken for IT deployment in the changing operational environment and to integrate new technology with the delivery process. It has been proposed to reduce the number of data centres. The challenge is to reduce them to 100 from 770 after consolidation, and the network operations centre from 65 to 25 in number.[16] Such ideas have been put on the table because the administration has become aware of the strength of the cloud systems. The US military is expecting to save up to 30 per cent of the IT budget by 2016 once cloud computing architecture is adopted. It would further reduce the cost of training required to maintain IT infrastructure and applications. The intelligence is expected to be improved by interlinking remote databases.[17] The cloud computing strategy targets to achieve objectives such as reduced costs and increased IT service delivery efficiencies, increased mission effectiveness and enhanced cyber security.[18] The DoD has contracted Lockheed Martin, IBM, HP Enterprise Services, General Dynamics, Northrop Grumman, MicroTech and Criterion Systems to create the Army Private Cloud.[19]

The IT modernization targets are likely to be achieved through cyber-secure cloud environment under the framework of Joint Information Environment (JIE).[20] The JIE is a robust and resilient enterprise that delivers faster, better-informed collaboration and decisions enabled by secure, seamless access to information regardless of computing device or location. The DoD enterprise cloud environment is a key component to enable the department to achieve JIE goals.

**Cloud Computing in China's People's Liberation Army (PLA)**

The Chinese government has been highly supportive of the cloud computing industry under the aegis of National Development and Reform Commission (NDRC), the Ministry of Industry and Information Technology (MIIT) and the Ministry of Finance (MoF). The 'Auspicious Cloud Project' was launched in 2010, aimed at developing chip designs, hardware, network, operators, terminals and a variety of other cloud applications.[21] China is developing cloud computing technology for a wide range of private sector, civilian, military and government uses. The government is keen to invest in the technology for its IT systems, with the goal of modernization of the PLA. The military is aware of the benefits of cloud computing and it is likely that military cloud computing

technology will see greater use in the PLA in the years to come. Although the PLA is yet to deploy military cloud at the broad level, it appears to be in the development phase. The General Staff Department's 61st Research Institute is actively conducting research into military cloud computing.[22]

### Cloud Computing in United Kingdom (UK) Ministry of Defence (MoD)

The UK government intends to establish a cloud computing approach (the G-Cloud) to provide services across departments for common corporate functions such as human resource and finance. The government has come out with its ICT strategy which has identified cloud as a key component. The strategy document states that the updates to the defence network and wider ICT must consider migration towards cloud computing, in particular the G-Cloud. Furthermore, it calls for need to define a defence platform as a service framework to allow the development of standard and interoperable solutions.[23]

### Cloud Computing in Australia's DoD

The Department of Finance and Deregulation of the Australian government has published the *Cloud Computing Policy* document. The national cloud computing strategy identifies that the Australian government, with an annual procurement of over US$ 5 billion in ICT and associated services, has a role in providing leadership on the appropriate adoption of cloud computing and in the flow on effect from terms and products procured by the government to other organizations in the economy.[24] The Australian DoD is reducing its number of computer rooms from 280 to 10, and plans to move into more of a private cloud, virtualized environment, which provides more flexibility as well as the ability to scale the capacity up faster than at present.[25] Though the department does not currently use cloud services to any significant extent due to security reasons, it holds the view that the current Copyright Act is inadequate to allow full usage of cloud computing advancements in the military.[26]

## Cloud Computing and India

To harness the benefits of cloud, Government of India's Department of Electronics and IT (DeitY) has taken up an ambitious project termed 'GI Cloud'. This is an initiative to leverage cloud computing for effective

delivery of eServices. The DeitY has prepared a multipronged strategy to adopt cloud computing and has set up a GI Cloud Task Force and a Cloud Working Group and published two reports. The *GI Cloud Strategic Direction Paper* highlights the key government ICT infrastructure components that are already in place to act as the building blocks. The *GI Cloud Adoption and Implementation Roadmap* talks about the 'GI Cloud Ecosystem' and identifies the major actors, their activities and roles. As a partner to this process, the National Association of Software and Services Companies (NASSCOM, established in 1988), in consultation with industry members and DeitY, is expected to finalize these reports and collaborate further on this project.[27]

Also, the Centre for Development of Advanced Computing (CDAC) has established a private cloud environment to offer basic cloud services such as infrastructure, platform and software service to government and small and medium enterprises. The Centre has developed an open-source free software suite called 'Meghdooth',[28] which converts data centre to cloud centre and offers value-added features for porting of e-governance applications.[29] To harness the benefits of cloud, the 'GI Cloud', a cloud computing environment, will be used by government departments and agencies at the centre and states for on-demand programming, testing platforms and software and data services.[30] The department rolled out the national cloud initiative, 'Meghraj', on 4 February 2014,[31] to address the demand of a secure unified cyberspace to deliver government services and optimal utilization of shared IT infrastructure and resources.[32]

The present pattern of investments into cloud appears to be more of civilian and commercial-centric; the defence sector is yet to articulate its requirements from cloud computing. Table 2 summarizes strategies of various states just discussed.

**Table 2** Summary—Cloud Computing Strategy

| *Country* | *Defined Cloud Computing Policy/Strategy* | | *Agencies Involved in Research/ Development* | *Comments* |
|---|---|---|---|---|
| | *Government* | *Defence* | | |
| US | 2010 | 2012 | National Institute of Standards and Technology.<br>Defense Information Systems Agency. | |

| *Country* | *Defined Cloud Computing Policy/Strategy* | | *Agencies Involved in Research/ Development* | *Comments* |
|---|---|---|---|---|
| | *Government* | *Defence* | | |
| UK | 2011 | No | Government Digital Services | Cloud Computing for MoD is part of government cloud strategy. |
| Australia | 2013 | No | Australian Government Information Management Office Defence Signals Directorate. Australian Academy of Technological Sciences and Engineering. | The *Australian Government Cloud Computing Policy* of 2013 supersedes the April 2011 Australian government's *Cloud Computing Strategic Direction Paper*. |
| China | No | No | General Staff Department's 61st Research Institute. | There are no indications that China has set out a singular military-wide cloud computing solution. |
| India | No | No | Department of Electronics and Information Technology Centre for Development of Advanced Computing. | The Government of India's *GI Cloud (Meghraj) Strategic Direction Paper* and implementation roadmap were published in April 2013. |

## Challenges in Adopting Cloud Computing

Cloud computing technology poses many challenges from security point of view and there are some potential risks which need to be analysed and addressed before any cloud model is adopted. The cost of transition from existing software and data to the cloud may be high and technically

challenging; the issue of interoperability arises when applications are to be moved to a different service provider and since architectures vary, there is an associated cost of porting data and applications. Since cloud computing encapsulates information along with infrastructure, information assurance is of utmost importance. In the military context, information has different sensitivity requirements and falls under various categories such as classified and mission-specific intelligence to publicly available communication and recruitment information. There are various types of information that have to be managed when opting for cloud services: personal information; patent/trade secret; customer information; corporate information; medical information; and financial information. The data needs sensitivity classification for security controls.[33] The controls thus employed prevent unauthorized access during storage as well as in transit. An audit mechanism thereafter ensures that data security controls are enforced according to the best practices.

A major challenge in the adoption of cloud as a key infrastructure is the security concerns associated with it. The cloud, in its different deployment models, is vulnerable to data breaches, data loss and leakage, credential theft or misuse, insecure interfaces, denial-of-service (DoS) attacks and so on.[34] The cloud inherits the vulnerabilities from all the underlying technologies. The organizations adopting cloud have to understand the operational environment, while a risk assessment exercise has to be carried out in order to understand the implications of threats to the business processes. The associated risk varies from implementation or integration to interoperability, data loss and privacy risk to intellectual property theft risk and security to contractual complexities. It is a complex function of data sensitivity, security architecture at the provider and organizational ends, deployment model of the cloud, disaster recovery plan, legislative mechanism, service-level agreements (SLA) obligations, among others. Moreover, the users of cloud have limited control over the location of data storage and computation which could lie under different legal jurisdictions.[35] In the case of cloud, the data storage, processing and transmission takes place beyond the physical borders of a nation-state and the lack of an international legal framework adds to the existing concerns.

Various new developments in the cloud field are constantly taking place. The industry is trying to overcome the existing limitations of this technology. A cognitive computing cloud platform has been developed by IBM, known as Watson. This technology intends to bring together unique and varying sources of data, including general knowledge, industry-

specific content and subject matter expertise. The Watson Ecosystem can interact in natural language where users can pose questions and get answers back with links to the relevant content from Watson's database.[36] This technology, once integrated with cloud, has vast potential for defence applications due to ease of interface in natural language, analytics and cognitive computing. The defence operations are data intensive and analytics can identify the patterns, thereby bringing in efficiency and precision in decision making, both strategic and tactical.

## CONCLUSION

Cloud computing technologies have succeeded in building an important computing platform for multidisciplinary utility. This platform has inspired formation of a new architecture for various systems which have significant data dependence. It has allowed people to think differently and develop ecosystem of tools for multiple utilities. In a relatively short span of time, cloud computing has found applicability in various arenas of relevance from social to strategic fields: e-governance, health care, education, public distribution systems and defence.

Presently, in the defence sector, it has been observed that cloud computing is mainly being viewed as an alternate to existing IT systems. Few states are found juxtaposing this system with their existing ICT infrastructure. Particularly, defence training is one arena where cloud computing demonstrates major relevance in its present form. In the minds of defence planners, there is some form of uncertainty with regard to adapting to cloud computing completely. Defence agencies have concerns due to issues concerning mission criticality and classified nature of data pertaining to national security interests.

It is important to appreciate that cloud computing has tremendous utility for the armed forces and display of any rigid security apprehension would eventually only limit the armed forces from exploiting this technology to its fullest potential. Reluctant defence forces could make a beginning by opting for non-classified or non-mission critical applications and for battlefield-specific, information-intensive applications for personnel on the ground. It is expected that as the research into secure defence applications of cloud computing intensifies, the reluctance in adopting cloud as an alternative to traditional IT solutions will reduce. In the foreseeable future, cloud computing will not displace existing IT solutions totally, rather it will complement existing technologies and offer an increased number of options. Astute investment into cloud computing

would revolutionize the ICT set-up of the armed forces. It would help them to improve accessibility and make their warfighting platforms more skilful because of the real-time availability of inputs about various variables, and would also make the soldier more aware about his/her surroundings. Additionally, adopting cloud computing would cut down capital costs due to reduction in the spending on technology infrastructure.

## Notes

1. Mell, Peter and Grance, Timothy, 'The NIST Definition of Cloud Computing', Special Publication 800-145, National Institute of Standards and Technology, US Department of Commerce, September 2011, p. 2; for more details, see http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf, accessed 1 October 2013.
2. Ibid.; see also Huth, Alexa and Cebula, James, 'The Basics of Cloud Computing', US-CERT, pp. 2–3, available at http://www.us-cert.gov/sites/default/files/publications/CloudComputingHuthCebula.pdf, accessed 1 October 2013. Also, refer to http://www.cloud-competence-center.com/understanding/cloud-computing-service-models/, accessed 10 November 2013.
3. Zissis, Dimitrios and Lekkas, Dimitrios, 'Addressing Cloud Computing Security Issues', *Future Generation Computer Systems*, Vol. 28, 2012, p. 1, available at http://www.cse.msstate.edu/~dampier/cse8993/zissis%20and%20lekkas.pdf, accessed 2 October 2013.
4. Crozier, Ry, 'Defence Views Copyright as Barrier to Cloud', *itnews* (Sydney), 19 December 2012, available at http://www.itnews.com.au/News/326854,defence-views-copyright-as-barrier-to-cloud.aspx, accessed 18 October 2013.
5. Mathur, Sandeep, 'Moving to Cloud can be Smart Decision for Governments and Companies', *The Economic Times* (New Delhi), 7 May 2013, available at http://articles.economictimes.indiatimes.com/2013-05-07/news/39091309_1_cloud-computing-public-cloud-cloud-strategy, accessed 2 October 2013.
6. Columbus, Louis, 'Predicting Enterprise Cloud Computing Growth', *Forbes* (New York), 4 September 2013, available at http://www.forbes.com/sites/louiscolumbus/2013/09/04/predicting-enterprise-cloud-computing-growth/; also, see 'Cloud Computing Market Revenue to Approach $20 Billion by End of 2016', *PR Newswire* (New York), 20 August 2013, available at http://www.prnewswire.com/news-releases/cloud-computing-market-revenue-to-approach-20-billion-by-end-of-2016-according-to-new-451-research-study-220322891.html, accessed 2 October 2013.
7. Gordon, Joanna, Hayashi, Chiemi, Elron, Dan, Huang, Lin and Neill,

Renee, *Exploring the Future of Cloud Computing*, Switzerland: World Economic Forum, 2010, p. 2, available athttp://www3.weforum.org/docs/WEF_ITTC_FutureCloudComputing_Report_2010.pdf, accessed 2 October 2013.

8. Fischer, Eric A. and Figliola, Patricia Moloney, 'Overview and Issues for Implementation of the Federal Cloud Computing Initiative', *Congressional Research Service*, 2013, p. 9, note R42887, available at http://www.fas.org/sgp/crs/misc/R42887.pdf, accessed 4 October 2013.
9. Linthicum, David, 'How and Why the Military should Adopt the Cloud', 14 May 2010, available at http://www.infoworld.com/d/cloud-computing/how-and-why-the-military-should-adopt-the-cloud-484, accessed 4 October 2013.
10. Spalding, Robert S., 'Cloud Computing and the New Age of War', Air War College, United States Air Force, p. 7, available at http://www.au.af.mil/au/awc/awcgate/cst/bh2009_spalding.pdf, accessed on 9 March 2014.
11. The US Department of Defense, 'Cyber Security and Reliability in a Digital Cloud', January 2013, p. 7, available at http://www.acq.osd.mil/dsb/reports/CyberCloud.pdf, accessed 6 October 2013.
12. The Autonomous Real-Time Ground Ubiquitous Surveillance Imaging System (ARGUS-IS) has a video sensor which produces 1.8 billion pixels per frame at 12 frames per second, providing continuous coverage of an area up to 100square kilometre area. A single ARGUS-IS class sensor can produce more than a petabyte of data per day. Processing video data from sensors such as ARGUS-IS requires stitching the images from the individual cameras, rectifying the data according to known geographic references, removing the effects of motion by the airborne platform, modelling the unchanging background, detecting and tracking vehicle motion, selectively compressing the raw data and archiving the results. This processing chain might require 100 operations per pixel.
13. Accenture, *A New Era Cloud Ushers in Insight-driven Defense*, pp. 9–10, available at http://www.accenture.com/SiteCollectionDocuments/PDF/Accenture-New-Era-Cloud-Ushers-in-Insight-Driven-Defense.pdf, accessed 6 October 2013.
14. Exploratory security analytics is a cloud-driven tool that enables defence agencies to track and model the activities, motivations and behaviours of their cyber adversaries, and to use this intelligence to anticipate emerging threats and take proactive actions to head them off. The scale and processing power needed to support these tools means that the cloud is the only viable and cost-effective environment in which to run them.
15. Lockheed Martin and Market Connections Inc., 'Getting Secure in the Cloud', July 2011, p. 5, available at http://www.lockheedmartin.com/

content/dam/lockheed/data/corporate/documents/Getting-Secure-in-the-Cloud.pdf, accessed 6 October 2013.

16. Takai, Teri, *DoD CIO's 10-Point Plan for IT Modernization*, Washington, DC: US Department of Defense, 2012, pp. 4–6, available at http://dodcio.defense.gov/Portals/0/Documents/ITMod/CIO%2010%20Point%20Plan%20for%20IT%20Modernization.pdf, accessed 1 October 2013.
17. Tanaka, Edward, 'The NSA and Military Cloud Computing', 27 January 2012, see http://www.patexia.com/feed/the-nsa-and-military-cloud-computing-just-painting-a-cyber-bullseye-for-attackers-2401, accessed 8 October 2013.
18. The US Department of Defense, 'Cloud Computing Strategy', July 2012, p. 4, available at http://www.defense.gov/news/dodcloudcomputingstrategy.pdf, accessed 8 October 2013.
19. Montalbano, Elizabeth, 'Army Awards $250 Million Cloud Contract', *InformationWeek* (New York), 9 January 2012, available at http://www.informationweek.com/government/cloud-saas/army-awards-250-million-cloud-contract/232301444, accessed 12 October 2013.
20. Kenyon, Henry S., 'Joint Information Environment is Under Way', 16 September 2013, available at http://www.afcea.org/content/?q=node/11696, accessed 25 November 2013.
21. 'China's Cloud Computing Strategy', *Hong Kong Trader*, 5 June 2013, available at http://www.hktdc.com/info/mi/a/hkthk/en/1X09TCME/1/Hong-Kong-Trader-Hong-Kong-Edition/China-S-Cloud-Computing-Strategy.htm, accessed 24 October 2013.
22. Ragland, Leigh Ann, McReynolds, Joseph, Southerland, Matthew and Mulvenon, James, 'Red Cloud Rising: Cloud Computing in China', Research Report prepared on behalf of the US–China Economic and Security Review Commission, Centre for Intelligence Research and Analysis, 5 September 2013, p. 38, available at http://china.usc.edu/App_Images//uscc-2013-china-cloud-computing.pdf, accessed 18 October 2013.
23. The UK MoD, 'Defence ICT Strategy', No. 1.00, 29 October 2010, p. 26, available at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/27373/modict_strategyv1.pdf, accessed 18 October 2013.
24. Department of Finance and Deregulation of the Australian Government, *Australian Government Cloud Computing Policy*, Version 2.0, May 2013, p. 4, available at http://agimo.gov.au/files/2012/04/Australian-Government-Cloud-Computing-Policy-Version-2.0.pdf, accessed 18 October 2013.
25. Connolly, Byron, 'Interview: Dr Peter Lawrence, CIO, Department of Defence', *CIO* (Sydney), 4 February 2013, available at http://www.cio.com.au/article/452683/interview_dr_peter_lawrence_cio_department_defence/, accessed 18 October 2013.

26. Crozier, 'Defence Views Copyright as Barrier to Cloud'.
27. Available at http://www.nasscom.in/government-india%E2%80%99s-cloud-initiative?fg=248518, accessed 24 November 2013.
28. Meghdooth offers various features in cloud environment such as platform and infrastructure as a service (PaaS and IaaS), on-demand dynamic provisioning, metering and monitoring, graphical installation of middleware stack, Web-based management of cloud resources, provision for deployment of multi-instance user appliances, customized elasticity, Web service-based management of cloud, high availability and enhanced security across layers.
29. CDAC, 'Cloud Computing at CDAC', available at http://cdac.in/index.aspx?id=cloud_ci_cloud_computing, accessed 12 October 2013.
30. DeitY, Government of India, *Government of India's GI Cloud Strategic Direction Paper*, April 2013, p. 4, available at http://deity.gov.in/sites/upload_files/dit/files/GI-Cloud%20Strategic%20Direction%20Report%281%29.pdf, accessed 24 October 2013.
31. See 'Shri Kapil Sibal Launches 'National Cloud' Under "Megh Raj"', available at http://pib.nic.in/newsite/PrintRelease.aspx?relid=102979; and https://cloud.gov.in/, accessed on 21 March 2014.
32. Srivastava, Moulishree, 'Cloud Computing: Govt. to Roll Out "Meghraj" in December', *Livemint* (New Delhi), 29 October 2013, available at http://www.Livemint.com/Industry/RN7yyjLwbeV66tPCXfrJUM/Cloud-computing-Govt-to-roll-out-Meghraj-in-Dec.html, accessed 27 November 2013.
33. Deloitte, 'Cloud Computing: Forecasting Change', p. 22, available at https://www.deloitte.com/assets/Dcom-Global/Local%20Assets/Documents/TMT/cloud_-_market_overview_and_perspective.pdf, accessed 22 October 2013.
34. Samson, Ted, 'Top 9 Threats to Cloud Computing Security', *Infoworld*, 25 February 2013, available at http://www.infoworld.com/t/cloud-security/9-top-threats-cloud-computing-security-213428?page=0,1, accessed 9 March 2014.
35. The PATRIOT Act in the US applies to all data held by all US companies, irrespective of the location of the data.Department of Innovation Industry, Science and Research—Australian Government, 'Cloud Computing—Opportunities and Challenges', October 2011, p. 17, available at http://www.innovation.gov.au/Industry/InformationandCommunicationsTechnologies/ITIIC/Documents/CloudComputingOpportunitiesandChallenges.pdf, accessed 22 October 2013.
36. 'Announcing the IBM Watson Ecosystem Program', available at http://www-03.ibm.com/innovation/us/watson/index.shtml, accessed 27 November 2013.