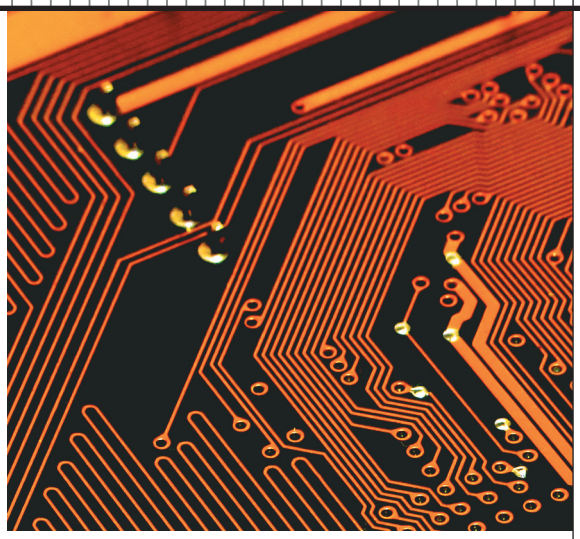
Cloud Computing in Developing Economies



Nir Kshetri
University of North Carolina—Greensboro

The developing world must exploit the opportunities afforded by cloud computing while minimizing the associated risks to allow access to advanced IT infrastructure, data centers, and applications and protect sensitive information.

The developing world's cloud computing sector has received considerable attention from global and local IT players, national governments, and international agencies. For example, IBM has established cloud computing centers in China, India, Vietnam, Brazil, and South Korea. Other global cloud players such as Microsoft, VMware, Salesforce, Dell, and Parallels are actively searching for opportunities in the developing world. Perhaps even more impressive is that developing-world-based firms have jumped on the cloud bandwagon. Cloud-related venture capital and other investments are also flowing into developing economies. It is probably fair to say that in no other major technological innovations has the developing world received this level of attention.

However, findings and conclusions about the potential and impact of cloud computing in the developing world drawn from surveys, studies, and experiences of companies are confusing and remarkably inconsistent. Some analysts suggest that developing countries will be attractive markets for cloud services and predict that this technology will soon make "healthcare 2.0," "banking 2.0," and "education 2.0" realities in these countries.[1]

In theory, developing economies could catch up with developed countries as the cloud gives them access to the same IT infrastructure, data centers, and applications. The cloud arguably reduces infrastructure costs and levels the playing field for small- and medium-size enterprises (SMEs). In addition, software on the cloud would be easier to install, maintain, and update than client-based computing, which requires installing and configuring software and updating it with each new release, as well as revising other programs with every update.[2] Third, cloud services give users the flexibility of scaling up when demand increases.[3] Cloud proponents also argue that as software becomes free via Web-based applications or available in software as a service (SaaS), software piracy could decrease. A final but not secondary point concerns developing-world-based IT companies' domestic and international entrepreneurial activities in the cloud sector.

Little, if any, existing empirical evidence shows how effectively these theories, ideas, and speculations can translate into practice, however. A close look at the early stage of the cloud industry's development indicates that these observations might underscore how economic and institutional problems remain central to the development and diffusion of information and communications technologies (ICTs) and entrepreneurial performance in the developing world. For one thing, the cloud is inherently linked to the multiple facets of data security.

Recent surveys suggest that many organizations are unprepared for their clouds' security. According to an April 2010 International Data Corporation (IDC) cloud computing poll conducted in Australia, China, Hong Kong, India, South Korea, and Singapore, fewer than 10 percent of the respondents were confident about their security measures.[4] Critics have also raised concerns about poor

Table 1. Current cloud computing application areas in developing countries.

Country	E-education	E-health	E-commerce/ e-business/ supply chain	E-governance	E-environment	Telecommuting
China	X	X	X		X	
East Africa	X					
India	X	X				
Korea			X			
Qatar	X					
South Africa			X			X
Turkey	X					
Vietnam	X			X		
West Africa					X	

bandwidth and a lack of forward and backward linkages. What is theoretically possible, versus what is practically achievable, is thus the critical issue.

STATE OF CLOUD COMPUTING IN DEVELOPING ECONOMIES

It's important to make clear at the outset that cloud computing in the developing world is in its infant stage. Studies have indicated a lack of cloud awareness, even among large companies. According to a 2009 Gartner survey of large enterprises, half the respondents in emerging markets either hadn't heard of cloud computing or didn't know what it was.[5]

IT-intensive areas such as offshoring and software development are enthusiastically embracing clouds. In India, cloud demand is high in the offshoring industry and technology hubs. In South Africa, the call center industry has been the fastest growing area for the cloud. Likewise, the IBM Cloud Center in China's Wuxi City targets software developers.

The market for the cloud in developing countries is small but expanding rapidly. An IDC study suggested that emerging markets such as Brazil, Russia, India, and China will likely be important forces driving the global shift toward the cloud,[6] with China and India having the greatest mid- to long-term potential for the cloud. The report also predicted that the Indian SaaS market would experience a compound annual growth rate of 77 percent during 2006-2010. India's National Association of Software and Services Companies and McKinsey estimated that remote infrastructure management will be a US$15 billion industry in India by 2013.

Cloud-related activities in the developing world are mainly concentrated in big economies such as China, India, Brazil, South Africa, and Vietnam. Nonetheless, the cloud is gradually making an inroad into smaller economies, as Table 1 illustrates. Dell reported that it might offer cloud services in Saudi Arabia and other Middle Eastern countries by the end of 2010. Likewise, in April 2010, Microsoft and Qatar Telecom (Qtel) signed a strategic alliance to offer cloud-based services, applications, and devices over Qtel's network. Kenyan companies are also showing interest in the cloud.[7]

Application areas

Table 1 lists some cloud application areas currently being explored in developing economies.

E-education. E-education has received particular attention. The Computational Intelligence Research Group at the University of Pretoria, South Africa, uses the cloud for next-generation medical research. University students use the cloud to conduct research in the development of drugs for the treatment of Africa-specific serious illnesses.

In East Africa, the Higher Education Alliance for Leadership through Health (Health Alliance), a consortium of seven universities (universities in Kenya, Jimma University in Ethiopia, the University of Kinshasa in the Democratic Republic of Congo, Muhimbili University of Health and Allied Sciences in Tanzania, and Makerere University in Uganda), is working with industry experts to extend education through virtual computing labs that students access remotely.

Universities in China, Qatar, and Turkey are among the 17 educational institutions worldwide participating in the IBM Cloud Academy, which allows access to a range of educational resources. In addition, Chinese universities can access a supercomputer to analyze data on disease-spread patterns and climate changes. Likewise, Indian universities are banking on the cloud to develop innovative research and education activities. The Indian Institute of Technology, Kanpur, and other academic institutions have also adopted the cloud.

Although less well known in the global IT map, Vietnam has recently come into the limelight due to its contributions to development of the cloud, especially in e-education. Vietnamese government institutions and universities use

the cloud to develop education programs. Vietnam National University (VNU) has established a cloud platform. IBM and VNU have signed a memorandum of understanding about using the cloud to build IT skills.

E-health. Another visible application of the cloud is in healthcare. India's ICICI Bank's insurance arm has used Zoho's Web-based applications to develop services such as personalized insurance for patients with diabetes. The company adjusts premiums based on how well policyholders stick to a fitness plan.[1]

Likewise, in May 2009, IBM opened a Healthcare Industry Solution Lab in Beijing. The lab will work with hospitals and rural medical cooperatives. The Guang Dong Hospital of Traditional Chinese Medicine has implemented a suite of healthcare data-sharing and analytics technologies, known as Clinical and Health Records Analytics and Sharing. CHAS combines input from traditional Chinese medicine and modern Western medicine. Hospitals use CHAS to share electronic medical records (EMRs) incorporating this data across the hospital network.

E-commerce, e-business, and supply chain. Yet another major application of the cloud has been in e-commerce and supply-chain management.

In China, IBM's pilot project Yun (Chinese for "cloud") lets businesses select and implement cloud services. The platform dynamically allocates storage, server, and network resources without human input.

The Wang Fu Jing department store, one of China's largest retailers with more than 10 million customers, has deployed cloud computing in supply-chain management, which it uses to share information with its network of retail stores and implement business-to-business e-commerce.

In Korea, banking, telecommunications, and IT hosting services use the cloud; while in South Africa, Nedbank is automating its business processes through the cloud.

Emerging application areas. Emerging application areas in developing countries include e-government, e-environment, and telecommuting.

Vietnam's Ministries of Education and Training, Science and Technology, and Information and Communications have jointly developed cloud-based academic programs that offer computing courses, free software tools, and business case studies.

In China, scientists have access to a supercomputer that lets them analyze climate change data. In West Africa, the UK's Hadley Center for Climate Prediction and Research is negotiating with Amazon to sponsor a researcher for free access to cloud services.

South Africa is a leader in using the cloud to support telecommuting. Call center agents and software developers can log in from anywhere using IP lines or a virtual private network (VPN).

Supporting trends

Several trends facilitate the cloud's diffusion in developing countries.

Multinationals' search for opportunities. The activities of several companies triggered the cloud industry's evolution in the developing world. In 2008, IBM opened a cloud center in Bangalore, India, that targets mid-market vendors, universities, government bodies, and microfinance and telecommunications companies. That same year, IBM opened a similar center in Beijing. Cloud computing is also a primary R&D area in its China's Shanghai facility. In addition, IBM has built data centers to offer cloud services in Johannesburg, South Africa, and Hanoi, Vietnam.

Vietnam and China are notable examples of economies that have meaningful government interventions in the cloud sector.

Microsoft's cloud offerings in developing countries include the Business Productivity and Online Suite (BPOS), Windows Azure (a platform for building, deploying, and selling applications on the cloud), and an infrastructure suite to build private and public clouds. Developers in Malaysia, India, and China can use Visual Studio 2010, launched in April 2010, to build applications for Azure. BPOS, which consists of e-mail, live meeting, and collaboration tools, was launched commercially in India in November 2009 and by April 2010 had 15,000 users in 600 organizations.[8]

Salesforce, which started its operations in India in 2005, focuses on major cities and is creating cloud awareness through its SaaS products. Its customer base in India grew by 42 percent during its fiscal year ending in January 2010.

By mid-2009, VMware was active in developing economies such as India and South Africa. Likewise, the US company Parallels announced a plan to establish cloud operations in India. Similarly, Computer Sciences Corporation announced that it would develop its Vietnamese operation as a cloud center. In the same vein, in July 2010, Japanese technology company NEC announced a plan to launch cloud services in China in 2011.

Governments' and international organizations' efforts. Vietnam and China are notable examples of economies that have meaningful government interventions in the cloud sector. Cloud computing in Vietnam is driven fundamentally by the government's belief that this technology will help the country build a skilled workforce, and universities, government ministries, and telecommunication vendors have adopted the cloud. One government agency uses the cloud to link government agencies, universities, private-sector research, start-ups, and other organiza-

tions.[9] Vietnam has been collaborating with IBM since 2007 on a pilot cloud program.

International agencies have facilitated cloud uses in some of the least developed countries. For instance, UNESCO and Hewlett-Packard have teamed up in the *brain gain initiative*, which harnesses the powers of the cloud and grid computing to slow brain drain in Africa and Arabic countries. The initiative gives researchers access to global scientific networks and computing power, letting them collaborate with experts around the world.[10] Burkina Faso's University of Ouagadougou launched two projects under the brain-drain initiative: modeling the movement of pollutants in the Sourou River drainage basin and implementing a high-performance computing grid. UNESCO and HP launched the initiative in five universities between 2006 and 2009. They plan to find partners and include 100 more universities by 2011.

Local firms' cloud-related entrepreneurial activities. Local firms have also contributed to the cloud's growth in developing countries.

Using virtualized resources lowers upfront investment and product development costs.

In 2009, the Brazilian firm Stefanini IT Solutions invested US$218,700 to boost cloud offerings. Similarly, China's Alibaba Group announced it would spend US$146 million in developing software, marketing, and establishing cloud centers that provide SaaS, especially to SMEs. The company expects to have 100 million online software users by 2011. Alisoft, Alibaba's software subsidiary, has captured more than 40 percent of China's SaaS market.[11] In September 2009, Alibaba also established a subsidiary focusing on the cloud. Also in that year, China Mobile announced a plan to launch BigCloud, a platform to enhance advanced mobile Internet and 3G experiences.

Some argue that India was an early entry in the cloud market because the country's huge data-processing centers served the world's big companies for on-demand computing. Wipro Technologies has built a private cloud for internal use. The company is also considering other services—for example, public clouds, hybrid clouds, and helping software vendors design and implement SaaS. Likewise, Tata Consultancy Services (TCS) is exploring the cloud's possibilities through pilot projects. Another Indian IT giant, Infosys, has partnered with major clients in cloud research. Other players, such as HCL Technologies and Bharti Airtel, are also embracing cloud computing.

Pressmart, based in Hyderabad, India, provides SaaS-based e-publishing and digitization services to the print industry. These services help firms deliver content across the Web and mobile networks through RSS, podcasts, blogs, social-networking sites, directories, and search engines. In 2008, the firm received venture capital investment from Draper Fisher Jurveston and NEA-IndoUS Ventures.

OPPORTUNITIES AFFORDED BY THE CLOUD

The cloud has opened a wide range of opportunities for users and developers in developing countries. Depending on their IT capabilities, firms can develop their own platforms or use applications on platforms provided by global players. Opportunities and prospects for the cloud, however, differ across economic sectors.

Access to IT infrastructure and applications

One of the most fascinating and important aspects of the cloud is that it lets businesses lease storage and computation resources as needed. The cloud could thus help overcome the small-size disadvantage and might provide opportunities for improving SMEs' welfare. Many recent examples from developing countries illustrate this point.

The cloud has let South African call centers lower capital investment because they don't need to own and maintain costly equipment. Thousands of call center agents have moved out of dedicated facilities and now can log in from anywhere using IP lines. Similarly, software developers work from home logging into the corporate VPN.[12]

The Chinese government-run IBM Cloud Center in Wuxi City's Science and Education Industrial Park in Jiangsu province also illustrates how clouds could help overcome small-size disadvantages. IBM provides technology including system *x* and system *p* servers on a secure virtual local area network. (It's worth noting that, on average, software firms in China have 25 employees; in India, the average is 174.)

Park tenants (mostly start-up software and chip-making companies) have access to an entire IT infrastructure. They don't need to buy servers, applications, or tools and pay only for the services they use. Using virtualized resources lowers upfront investment and product development costs. The industrial park plans to support "several hundred thousand developers across hundreds of companies."[9] In July 2009, IBM and Wuxi Park launched the PangooSky SaaS platform, which targets SMEs. Within a few weeks, 21 enterprises had signed agreements for the platform.

In another example, Vietnam Technology and Telecommunication offers server or storage capacity and system capability for its clients, which are mainly SMEs. VNTT's clients can expand these services as their needs grow. The company also plans to launch applications designed for construction and real-estate companies.

Productivity gains

Although no hard scientific evidence exists, anecdotes indicate that the cloud contributes to business productivity. For example, the South African call center industry has boosted productivity by as much as 20 percent.[12]

Similarly, India's Netmagic reports that its cloud services helped its clients cut costs by 25 to 30 percent, and Microsoft claims that its cloud services in India will help reduce costs by 10 to 50 percent.[13]

Cloud-related entrepreneurial activities

Cloud computing has opened opportunities for many organizations in the developing world to create and participate in the cloud ecosystem. AdventNet's Zoho division based in Chennai, India, is among notable success stories.[1] As noted earlier, Zoho operates a popular suite of Web-based applications used by hospitals and banks to offer specialized services. The suite had more than 2 million users in September 2009, 20 percent of whom were from India and China.[14]

India's Computational Research Laboratories is another high-profile cloud provider. In 2008, Yahoo signed a research pact with CRL in which Yahoo will use CRL's EKA supercomputer—the world's fourth fastest as of March 2009—to support cloud computing research.

Firms based in the developing world have also fostered international entrepreneurial capabilities. South Africa's Integr8 operates in Kenya, Nigeria, and Ghana and aims to expand to other African countries, where it plans to offer clouds and other hosted services. Other companies are acquiring foreign firms. For example, in April 2010, China's hiSoft Technology acquired the US cloud company Echo Lane.

Building applications on established cloud platforms

The cloud might play another equally important role by facilitating the development of applications on platforms provided by global players such as Microsoft and Salesforce.[1] Some argue that Indian companies especially are in a good position to provide software and services that run on the dominant cloud platforms. For example, Infosys, India's second-largest software exporter, has created a B2B solution for the auto sector on Azure.[8]

Developing new products and services

Another important opportunity for developing-world-based firms concerns the cloud's use in facilitating innovative products and services.

Consider the healthcare offshoring industry. Industrialized-world-based healthcare providers are offshoring services such as medical transcription, billing and insurance claims, teleimaging, and telepathology to India. Big companies dominate most of these services. The cloud will likely allow SMEs to participate in healthcare offshoring. Cloud applications such as those offered by Zoho reduce the up-front investments.

A final example of such an approach is the development of private cloud products based on Azure. About 4,000 applications have been built on Azure in India.[8] One small Indian firm, Wings Infotech, reportedly moved its enterprise resource planning and accounting services to Azure.[8]

Businesses and consumers have expressed distrust in the cloud and are cautious of using it to store high-value data or important personal information.

Opportunity to improve IT security

Countries differ in the deployment of security products. According to Europemedia, North America accounted for 58 percent of the 2002 global IT security market. Most organizations in the developing world lack IT security measures. According to one estimate, about 3 million SMEs in Brazil lacked antivirus software in 2006.[15] Likewise, in 2009, 60 percent of Kenyan banks were reported to have insecure systems.[16] Cloud computing could enhance security for these companies.

IT's *hollow diffusion* concept can be helpful in understanding a weak defense. Many companies in developing countries lack technological and human resources to focus on security. Hollow diffusion can be human-related (lack of skill and experience) or technology-related (failure to use security products).[17] Some ISPs in industrialized countries reportedly block content that originated from problematic networks in developing countries. In the cloud, economies of scale let third parties provide low-cost security for SMEs[17] that can address some of the security-related human concerns (for example, problems of installing and maintaining software) and technological issues.

CLOUD CHALLENGES AND RISKS

Some experts have raised concerns about data privacy and security associated with unauthorized access and use of information stored in the cloud for malicious purposes.[18] According to an October 2008 IDC report (http://blogs.idc.com/ie/?p=210), many organizations consider security concerns to be the most serious barrier to cloud adoption. Businesses and consumers have expressed distrust in the cloud and are cautious of using it to store high-value data or important personal information.

Cybercrime 2.0

Like healthcare 2.0, banking 2.0, and education 2.0, criminal practices on the Internet have upgraded to cybercrime 2.0. The cloud is a double-edged sword from the security standpoint. Despite the cloud's potential to provide low-cost security, small companies can increase security risks by storing sensitive data in the cloud.

Crimes target sources of value. Large company networks offer more targets to hackers. Cloud suppliers, which often are bigger than their clients, are attractive targets. More importantly, information stored in clouds is a potential goldmine for cybercriminals.

To understand a cloud's security risks, consider Google's 2009 report that it had discovered an attack on its infrastructures that originated in China.[19] The company further noted that the attack was part of a larger operation that infiltrated the infrastructures of at least 20 other large companies.

National and international security issues arise from the cloud's potential to be the ultimate spying machine.

One fear has been that attackers could steal intellectual property and other sensitive information stored in the cloud. Worse still, cloud providers might not notify their clients about security breaches. Evidence indicates that many businesses tend to underreport cybercrimes due to embarrassment, concerns about their credibility, and fear of dropping stock prices. A report from the Idaho National Engineering and Environmental Laboratory (www.us-cert.gov/control_systems/pdf/oil_gas1104.pdf) noted, "Many of the cyberattacks go unnoticed or may go unnoticed for long periods of time". Thus, an organization might never know that its intellectual property or other sensitive data in the cloud had been stolen.

Cloud providers and users face additional challenges in developing economies because of unfavorable institutional environments. In many developing countries, factors such as corruption, lack of transparency, and a weak legal system can exacerbate security risks.

Various aspects of the institutional environment can weaken the cloud's value proposition and discourage investors. In 2008, Google's CEO said that his company would work with Chinese universities, starting with Tsinghua University, on cloud-related academic programs. The country's unfavorable environment from the security standpoint, however, led to Google's withdrawal from China.

A final point concerns outage problems, which would worsen cloud computing's economics. Popular clouds such as Google's Gmail, Amazon's S3, and clouds belonging to Salesforce and Microsoft have all suffered outages.

The ultimate spying machine

National and international security issues arise from the cloud's potential to be the ultimate spying machine.

In April 2010, US- and Canada-based researchers published a report that tracked a sophisticated cyberespionage network, which they referred as the Shadow network.[19] The targets included the Indian Ministry of Defense, the United Nations, and the Office of the Dalai Lama. The report noted, "Clouds provide criminals and espionage networks with convenient cover, tiered defenses, redundancy, cheap hosting, and conveniently distributed command and control architectures."

Anecdotal evidence suggests that due to their increasingly important roles in national security, a high degree of protectionism characterizes many high-technology sectors. An atmosphere of suspicion and distrust among states can lead to such protectionism.

To capture the feelings accompanying intergovernmental distrust, consider the US and China trade and investment policy relationship. Chinese leaders are concerned about possible cyberattacks from the US. A deep-rooted perception among Chinese policymakers is that Microsoft and the US government spy on Chinese computer users through secret back doors in Microsoft products. Computer hardware and software imported to China from the US and its allies are subject to inspection. Chinese technicians control such imports and resist having Western experts install them, or closely monitor them if they do.[20]

Several years ago, Chinese cryptographers reportedly found an "NSA key" in Microsoft products, which they interpreted as pertaining to the US National Security Agency. The key allegedly gave the US government backdoor access to Microsoft Windows 95, 98, NT4, and 2000. Although Microsoft denied this allegation and issued a patch to fix the problem, Chinese officials remain unconvinced. Chinese leaders thus might be uncomfortable with storing data on clouds provided by foreign multinationals.

US policymakers are equally concerned about Chinese technology firms' internationalization. Some US lawmakers argue that Lenovo's acquisition of IBM's PC division could lead to a transfer of advanced technology to the Chinese government. When the US State Department was about to buy Lenovo computers in 2006, politicians and some commentators drew attention to the national security implications of placing Chinese computers into government offices. They argued that Lenovo's connections to the Chinese government could pose a threat.

Domestic security-related concerns also exist. Cloud computing will likely make it easier for governments to spy on citizens. An April 2010 Google report describes how

government authorities around the world ask the company to provide private information and to censor its applications.

Governments worldwide differ in how and how much they censor websites and use the Web for surveillance. Although more than 36 governments control the online environment, few have done so more skillfully than China. China's state strategies toward ICTs have sought to balance economic modernization and political control. China has pursued systematic, massive Internet surveillance. Tens of thousands of government agents reportedly engage in cybercontrol activities. According to the Berkeley China Internet Project, the Chinese government's censorship software hides websites containing phrases such as freedom, democracy, China-liberal, and falun, which means the "wheel of law" in Chinese Buddhism.[21] There were also reports that the Chinese government sent viruses to attack banned sites.[22]

If the recent major cyberespionage activities teach a lesson, it's that countries with strong cyberspying and cyberwarfare capabilities such as China will be in a good position to exploit the cloud's weaknesses for such activities. In the Shadow case, for instance, the cyberespionage network combined social-networking and cloud computing platforms, including those of Google, Baidu, Yahoo, Twitter, Blogspot, and blog.com, with traditional command and control servers.[19]

Negative country-of-origin effect

Cloud providers from developing countries such as China and India might face barriers to internationalization activities, particularly because security is among the most important concerns for cloud adoption. One concern is that the institutional environment in these countries can't guarantee the security and privacy of client data.

The prospect of civil and criminal prosecution is weak when security breaches and privacy violations occur in a country with a weak rule of law. Observers have noted that Indian cybercrime law and privacy enforcement are weak. European or US data protection laws, on the other hand, can't be enforced in India.

The Chinese government's reputation suggests that data stored in a cloud hosted in China might not be safe. These concerns further increase when taking into consideration the possibility of government control of China-based cloud providers. The state accounts for at least 70 percent of the economy and owns 76 percent of the country's wealth. For instance, mobile operators are 70 percent state-owned and are closely affiliated with the government. In 2001, in 70 percent of large- and medium-size corporate enterprises, boards of directors included Communist Party members. Consequently, Chinese companies tend to be more government-centric and less consumer-centric than Western companies. State priorities might thus supersede shareholders' profits for Chinese cloud providers. Partly due to real and perceived government control, China-based cloud providers might be perceived as less trustworthy and thus must combat the effects of negative country-of-origin images and stereotypes.

Criminal-controlled clouds

The cloud is potentially most vulnerable when viewed against the backdrop of criminal-owned clouds operating in parallel. The cloud can provide many of the same benefits to criminals as to legitimate businesses. Criminal-owned clouds might be used to effectively steal data stored in clouds.

Governments worldwide differ in how and how much they censor websites and use the Web for surveillance.

The well-known Conficker virus, which reportedly controls 7 million computer systems at 230 regional and country top-level domains and has a bandwidth capacity of 28 terabits per second, is arguably the world's biggest cloud and probably the most visible example of a criminal-owned cloud. As with legitimate cloud vendors, Conficker is available for rent. Cybercriminals can choose a location they want to rent on the Conficker cloud, pay according to the bandwidth they want, and choose an operating system. Customers have a range of options for the type of services to put in the Conficker cloud—launching a denial-of-service attack, spreading malware, sending spam, exfiltrating data, and so on.[23]

Insider risks

The cloud could also increase the exposure of organizational vulnerabilities to insider risks. Consider the offshoring industry, for example.

Security breaches and privacy violations associated with data leakage and abuse have been a major concern in the offshoring industry. Various anecdotes of data theft and misuse in Indian and Pakistani offshoring industries suggest that these fears are well founded. Consequently, offshoring firms have implemented preventive measures such as biometric authentication controls for workers; extensive monitoring and analysis of employee logs; and bans on cell phones, pens, paper, and Internet/e-mail access. Offshoring firms' computer terminals also lack hard drives, CD-ROM drives, or other ways to store, copy, or forward data.

In light of these problems, privacy and security concerns will be heightened if offshoring employees work

outside dedicated call centers, as many call center employees in South Africa do.

Risks to industrialized countries

It's tempting for global cloud players to use cheaper hosting services in developing countries. Cybercriminals, however, find it more attractive to target rich economies. For instance, the US is the number one target of cyberattacks. Because many developing countries are top cybercrime sources, security risks associated with the diffusion of clouds in these countries could spread to industrialized countries.

One area that has received particular attention is the escalation of economic and industrial espionage activities such as intellectual property theft. US government agencies such as the Department of Defense have reportedly been the targets and victims of such activities.[24] Likewise, between September 2004 and April 2005, more than a dozen versions of the Myfip worm were reportedly used to steal information such as CAD/CAM files containing mechanical designs, electronic circuit board schematics, and layouts from US businesses.[25] It's thus reasonable to expect that the cloud will allow an upgrade of these activities to industrial espionage 2.0.

There is much to be learned about the facilitators and inhibitors in the diffusion of cloud computing. An intriguing avenue for future research is to examine the effect of cloud computing and social media on concerns about security and privacy. Legitimate as well as illegitimate organizations and entities are exploiting the cloud to gain access to information about social media users through illegal, extralegal, and quasilegal means.

Future research might also examine how political, ethical, social, and cultural factors are associated with security issues in cloud computing. For instance, privacy and security issues of data stored on the cloud currently fall into a legally gray area. It is, however, reasonable to expect a gradual evolution of legal institutions as well as ethical and professional standards related to data stored on the cloud.

Countries could avoid some barriers to realizing the cloud's full potential through better planning and efforts to address human resources. Workers' existing skills might be insufficient for developing the cloud industry. Governments must take measures to develop cloud-related skills, and universities must provide hands-on experience.

The development of industries necessary for backward and forward linkages is equally important. The evolution of the cloud computing led telecommuting in South Africa, for instance, can be attributed to the country's high-speed, low-cost bandwidth. C

References

1. *The Economist*, "The Long Nimbus," 25 Oct. 2008, special section, pp. 15-17.
2. T.S. Parikh, "Engineering Rural Development," *Comm. ACM*, vol. 52, no. 1, 2009, pp. 54-63.
3. R.L. Grossman, "The Case for Cloud Computing," *IT Professional*, vol. 11, no. 2, 2009, pp. 23-27.
4. V. Yeo "'Instant Noodle' Mindset Undermines Cloud Security," ZDNet Asia, 30 June 2010; www.zdnetasia.com/instant-noodle-mindset-undermines-cloud-security-62201091.htm.
5. J. Burt, "Emerging Markets a Key for IT Hardware Vendors: Gartner," *eWeek.com*, 22 July 2009; www.eweek.com/c/a/IT-Infrastructure/Emerging-Markets-a-Key-for-IT-Hardware-Vendors-Gartner-667497.
6. R. Smith, "IDC Says IT Cloud Services To Reach $42 Billion By 2012," *Information Week*, 20 Oct. 2008, www.informationweek.com/blog/main/archives/2008/10/idc_says_it_clo.html.
7. P. Mwaniki, "Kenya; Out of the Blue, Here's the New Dot.com," *Daily Nation*, 14 Aug. 2009, www.nation.co.ke/News/-/1056/639700/-/ulo1o9/-/index.html.
8. S. Kannan, "Rising on the Cloud," *Hindu Business*, 19 Apr. 2010; www.thehindubusinessline.com/ew/2010/04/19/stories/2010041950100300.htm.
9. M. Cleverley, "Viewpoints: Emerging Markets: How ICT Advances Might Help Developing Nations," *Comm. ACM*, vol. 52, no. 9, 2009, pp. 30-32
10. SciDev.Net, "Africa; Plan to Slow the Brain Drain From Africa," *Africa News*, 23 Dec. 2009.
11. Alibaba Group, *Corporate Overview*, 2009; www.alibaba.com/aboutalibaba/aligroup/index.html.
12. R. Firth, "Use the Cloud to Work from Home," *ITWeb*, 13 Aug. 2009, www.itweb.co.za/sections/techforum/2009/0908130807.asp?S=Virtualisation&A=VRT&O=google.
13. P. Abrar, "Managed Services Spell Big IT Business," *The Economic Times*, 27 July 2009; http://economictimes.indiatimes.com/Infotech/Managed-services-spell-big-IT-business/articleshow/4823813.cms.
14. D. MacMillan, "Google, Zoho Challenge Microsoft Abroad, Too," *Businessweek*, 13 Sept. 2009; www.businessweek.com/technology/content/sep2009/tc20090911_644394.htm.
15. "SMBs in Brazil to Spend $260USM on IT Security in 2007," *BusinessWire*, 20 Nov. 2006.
16. K. Kinyanjui, "High Speed Internet Exposes Kenya to Cybercrime," *Business Daily*, 13 Aug. 2009; www.businessdailyafrica.com/-/539444/638794/-/rx1rgv/-/index.html.
17. C. Otis and P. Evans, "The Internet and Asia-Pacific Security: Old Conflicts and New Behavior," *Pacific Rev.*, vol. 16, no. 4, 2003, pp. 549-550.
18. L. McCreary, "What Was Privacy?" *Harvard Business Rev.*, vol. 86, no. 10, 2008, pp. 128-130.
19. Information Warfare Monitor/Shadowserver Foundation, *Shadows in the Cloud: Investigating Cyber Espionage 2.0*, Joint Report: Information Warfare Monitor Shadowserver Foundation, JR03-2010, 6 Apr. 2010; www.utoronto.ca/mcis/pdf/shadows-in-the-cloud-web.pdf.
20. J. Adams, "Virtual Defense," *Foreign Affairs*, vol. 80, no. 3, 2001, pp. 98-112.

21. N. Kshetri, "The Adoption of E-Business by Organizations in China: An Institutional Perspective," *Electronic Markets*, vol. 17, no. 2, 2007, pp. 113-125.
22. M.F. Guillén and S.L. Suárez, "Explaining the Global Digital Divide: Economic, Political, and Sociological Drivers of Cross-National Internet Use," *Social Forces*, vol. 84, no. 2, 2005, pp. 681-708.
23. R. Mullins, "The Biggest Cloud on the Planet Is Owned by ... the Crooks: Security Expert Says the Biggest Cloud Providers Are Botnets," *Network World*, 22 Mar. 2010; www.networkworld.com/community/node/58829?t51hb.
24. N. Kshetri, *The Global Cyber-crime Industry: Economic, Institutional and Strategic Perspectives*, Springer-Verlag, 2010.
25. N. Vardi, "Chinese Take Out," *Forbes*, 25 July 2005, p. 54.

Nir Kshetri *is an associate professor at the Bryan School of Business and Economics at the University of North Carolina–Greensboro. His research focuses on institutional and policy aspects of new technologies. Kshetri received a PhD in business administration from the University of Rhode Island. He is a member of the Southern Management Association. Contact him at nbkshetr@uncg.edu.*

cn **Selected CS articles and columns are available for free at http://ComputingNow.computer.org.**

"All writers are vain, selfish and lazy."

—George Orwell, "Why I Write" (1947)

(except ours!)

The world-renowned IEEE Computer Society Press is currently seeking authors. The CS Press publishes, promotes, and distributes a wide variety of authoritative computer science and engineering texts. It offers authors the prestige of the IEEE Computer Society imprint, combined with the worldwide sales and marketing power of our partner, the scientific and technical publisher Wiley & Sons.

For more information contact Kate Guillemette, Product Development Editor, at kguillemette@computer.org.

IEEE CSPress

www.computer.org/cspress